



Cisco HyperFlex Edge Deployment Guide, Release 3.0

First Published: 2018-04-24

Last Modified: 2019-08-21

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883



CONTENTS

CHAPTER 1	Technology Use Case	1
	Cisco HyperFlex Edge	1

CHAPTER 2	Preinstallation Checklist	3
	Single Switch Configuration	3
	Dual Switch Configuration	6
	Common Network Requirements	9
	HyperFlex Edge and Firmware Compatibility Matrix for 3.x Deployments	15
	Intersight Connectivity	16

CHAPTER 3	Installation	17
	Installation Overview	17
	Rack Cisco HyperFlex Nodes	18
	Cisco Integrated Management Controller Configuration	18
	Configuring CIMC: Static Assignment	18
	Configuring CIMC: DHCP Assignment	19
	Verifying Firmware Versions	20
	Deploying Cisco HX Data Platform Installer	21
	Configuring Your HyperFlex Cluster	21
	Verifying Cisco HX Data Platform Software Installation	27
	Cisco Intersight HX Installer for HyperFlex Edge	27

CHAPTER 4	Post Installation Tasks	29
	Post Installation Tasks Summary	29
	Create the First Datastore	29
	Configuring a Static IP Address for Live Migration and VM Network	31

(Optional) Post Installation Constrained Delegation	32
Configure Local Default Paths	33
Configuring a File Share Witness	34
Checking the Windows Version on the Hyper-V Host	40
Deploying VMs on a Hyper-V cluster	40
Install RSAT tools on the Management Station or Host	40
Managing VMs using Hyper-V Manager	44
Managing VMs using Failover Cluster Manager	45
Configuring HyperFlex Share to SCVMM	46
Re-enabling Windows Defender	48

CHAPTER 5**Appendix 49**

Sample Network Configurations	49
-------------------------------	----



CHAPTER 1

Technology Use Case

- [Cisco HyperFlex Edge, on page 1](#)

Cisco HyperFlex Edge

Introduction

Cisco HyperFlex Edge brings the simplicity of hyperconvergence to remote and branch office (ROBO) and edge environments. This document describes the deployment for HyperFlex Edge.

Limitations and Supportability Summary

Limitation for	Support
Cluster size and type	2-Node clusters: HX220c M5 Hybrid/HXAF220c M5 All-Flash Note 2-Node clusters require Intersight for initial deployment and ongoing management 3-Node clusters: <ul style="list-style-type: none">• HX220c M5 Hybrid/HXAF220c M5 All-Flash• HX220c M4 Hybrid/HXAF220c M4 All-Flash 4-Node clusters: HX220c M5 Hybrid/HXAF220c M5 All-Flash
Replication Factor	2 Note A reliable backup strategy is strongly recommended to ensure that production data is adequately protected.
Networking	1GE or 10/25GE networking without Cisco UCS Fabric Interconnects. HX Edge Systems do not implement QoS.

Limitation for	Support
HX clusters per vCenter	Up to 100



CHAPTER 2

Preinstallation Checklist

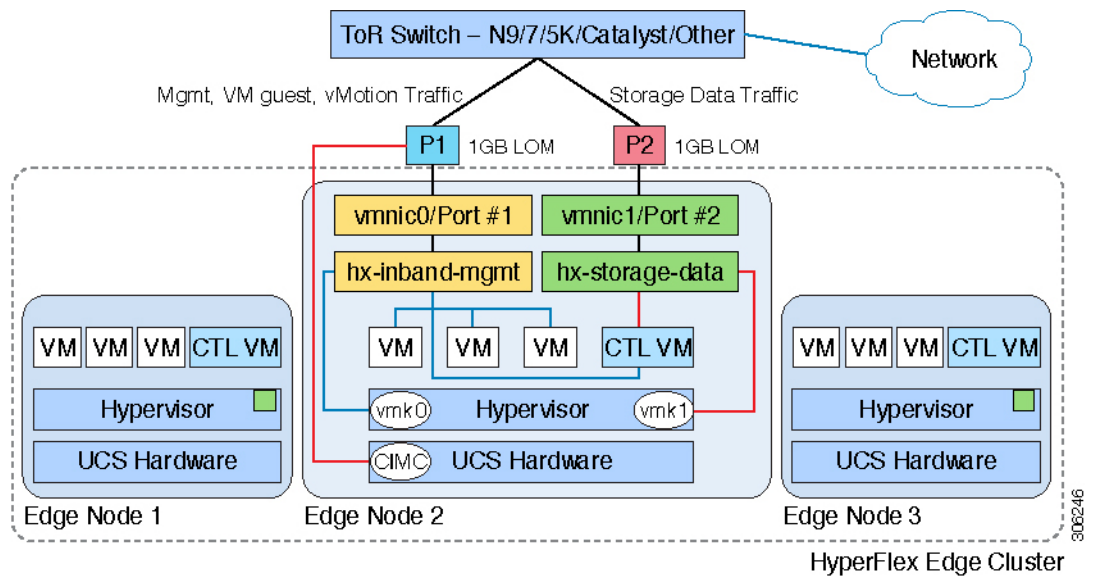
Select the preinstallation checklist for your deployment:

- [Single Switch Configuration, on page 3](#)
- [Dual Switch Configuration, on page 6](#)
- [Common Network Requirements, on page 9](#)
- [HyperFlex Edge and Firmware Compatibility Matrix for 3.x Deployments, on page 15](#)
- [Intersight Connectivity, on page 16](#)

Single Switch Configuration

Single switch configuration provides a simple topology requiring only a single switch, and two 1GE ports per server. Link or switch redundancy is not provided. Access ports and trunk ports are the two supported network port configurations.

Network Topology



Upstream Network Requirements

- A managed switch with VLAN capability
- Six physical 1GE ports for three HyperFlex nodes
- Jumbo frames are not required to be configured
- Portfast or portfast trunk should be configured on all ports to ensure uninterrupted access to Cisco Integrated Management Controller (CIMC)

Virtual Network Requirements

The recommended configuration for each ESXi host calls for the following networks to be separated:

- Management traffic network
- Data traffic network
- vMotion network
- VM network

The minimum network configuration requires at least two separate networks:

- Management network (includes vMotion and VM network)
- Data network (for storage traffic)

Two vSwitches each carrying different networks are required:

- **vswitch-hx-inband-mgmt**—ESXi management (vmk0), storage controller management, vMotion (vmk2), VM guest portgroups
- **vswitch-hx-storage-data**—HyperFlex storage data network, Hypervisor storage interface (vmk1)



Note

After some HyperFlex Edge deployments using the single switch configuration, it is normal to see the storage data vSwitch and associated portgroup failover order with only a standby adapter populated. The missing active adapter does not cause any functional issue with the cluster and we recommend leaving the failover order as configured by the installation process.

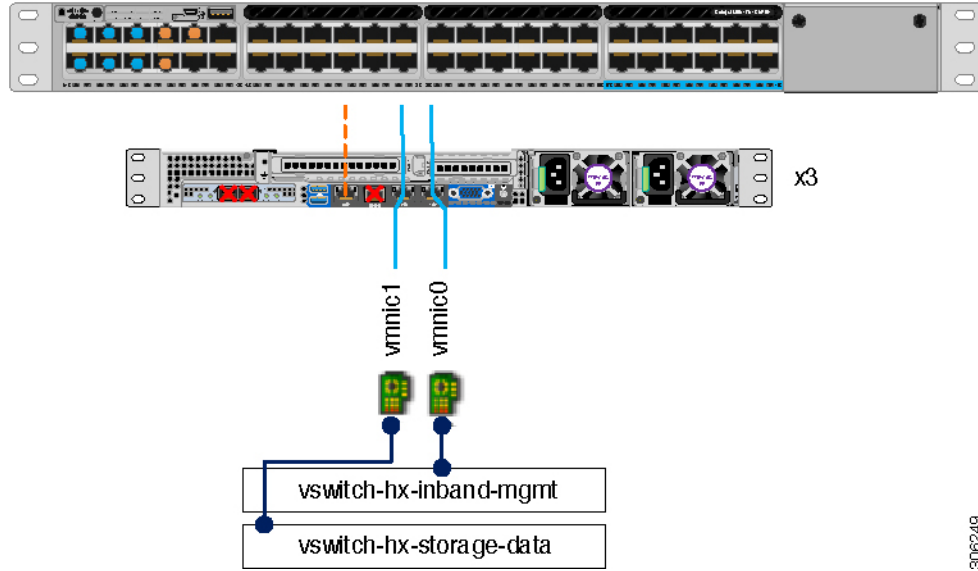
Port Requirements

Two 1GE ports are required per server:

- Port 1—management (ESXi and CIMC), vMotion traffic, and VM guest traffic
- Port 2—HyperFlex storage traffic
- There are two supported network port configurations: access ports or trunk ports.
- Spanning tree portfast (access ports) or portfast trunk (trunk ports) must be enabled for all network ports connected to HyperFlex servers.
 - Failure to configure portfast causes intermittent CIMC disconnects during ESXi bootup and longer than necessary network re-convergence during physical link failure.

- To decide if your deployment will use access ports or trunk ports, see the following section "About Access and Trunk Ports".

Physical network topology guidance:



- Cable both integrated LOM ports to the same ToR switch.
- If desired, cable the dedicated CIMC port to the same switch or to an out-of-band management switch.
- Do not use the 10GE ports on the VIC.

About Access and Trunk Ports

Ethernet interfaces can be configured either as access ports or trunk ports, as follows:

- An access port can have only one VLAN configured on the interface; it can carry traffic for only one VLAN.
- A trunk port can have one or more VLANs configured on the interface; it can carry traffic for several VLANs simultaneously.

The following table summarizes the differences between access and trunk ports. You can use the details described in this table to determine which ports to use for your deployment.



Important

Trunk ports are assumed in this guide, and is highly recommended for your deployment.

Trunk Ports	Access Ports
Requires more setup and definition of VLAN tags within CIMC, ESXi, and HX Data Platform Installer.	Provides a simpler deployment process than trunk ports.
Provides the ability to logically separate management, vMotion, and VM guest traffic on separate subnets.	Requires that management, vMotion, and VM guest traffic must share a single subnet.

Trunk Ports	Access Ports
Provides flexibility to bring in additional L2 networks to ESXi.	Requires a managed switch to configure ports 1 and 2 on discrete VLANs; storage traffic must use a dedicated VLAN, no exceptions.



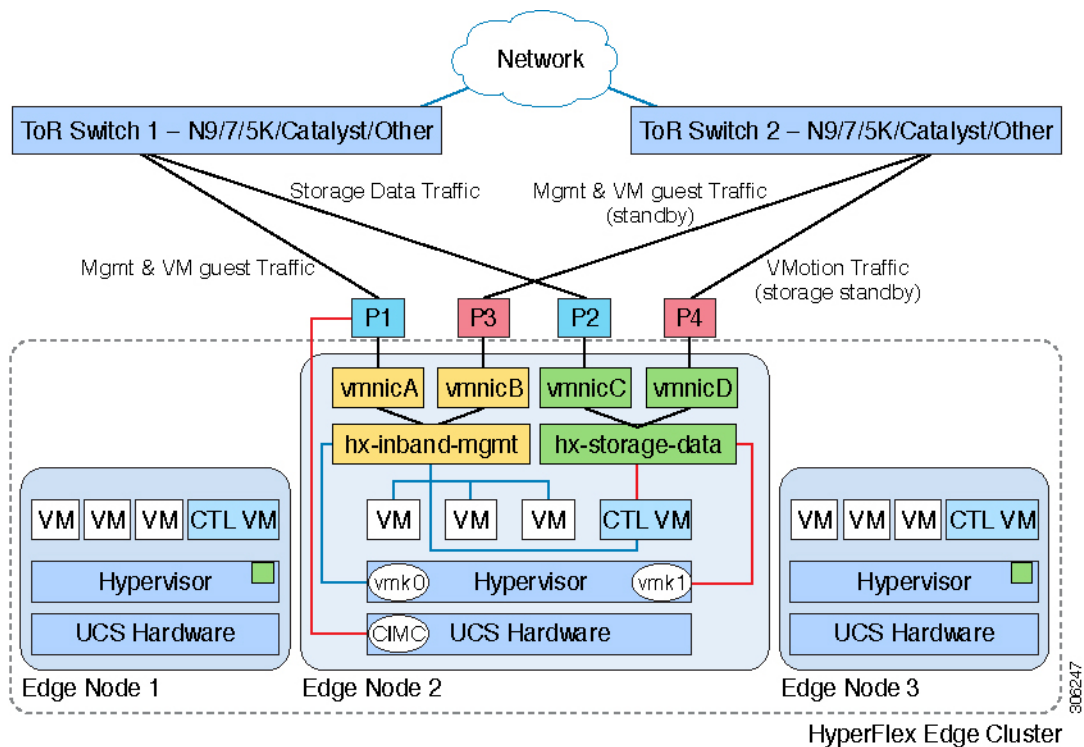
Note Both trunk and access ports require a managed switch to configure ports 1 and 2 on discrete VLANs.

See *Sample Network Configurations* for more details.

Dual Switch Configuration

Dual switch configuration provides a slightly more complex topology with full redundancy that protects against: switch failure, link and port failure, and LOM/PCIe NIC HW failures. It requires two switches that may be standalone or stacked, and four 1GE ports and one additional PCIe NIC per server. Trunk ports are the only supported network port configuration.

Network Topology



Upstream Network Requirements

- Two managed switches with VLAN capability (standalone or stacked)
- 12 physical 1GE ports for three HyperFlex nodes

All 12 ports must trunk and allow all applicable VLANs.

- Jumbo frames are not required to be configured
- Portfast trunk should be configured on all ports to ensure uninterrupted access to Cisco Integrated Management Controller (CIMC)

Virtual Network Requirements

The recommended configuration for each ESXi host calls for the following networks to be separated:

- Management traffic network
- Data traffic network
- vMotion network
- VM network

The minimum network configuration requires at least two separate networks:

- Management network (includes vMotion and VM network)
- Data network (for storage traffic)

Two vSwitches each carrying different networks are required:

- **vswitch-hx-inband-mgmt**—ESXi management (vmk0), storage controller management, VM guest portgroups
- **vswitch-hx-storage-data**—HyperFlex storage data network, Hypervisor storage interface (vmk1), vMotion (vmk2)

Failover order:

- **vswitch-hx-inband-mgmt**—entire vSwitch is set for active/standby. All services by default consume a single uplink port and failover when needed. Failover order for VM portgroups may be overridden as needed.
- **vswitch-hx-storage-data**—HyperFlex storage data network and vmk1 are set to the same active/standby order. The vMotion VMKernel port is set to use the opposite order when configured using the `post_install` script.

Port Requirements

Four 1GE ports are required per server:

- Port 1—management (ESXi, HyperFlex controller, and CIMC) and VM guest traffic
- Port 2—HyperFlex storage traffic (and vMotion standby)
- Port 3—VM guest traffic (and management standby)
- Port 4—vMotion traffic (and storage standby)
- Two ports using LOM and two ports from a PCIe add-in NIC:
 - 1 LOM and 1 PCIe port serve management and VM guest traffic in a redundant configuration

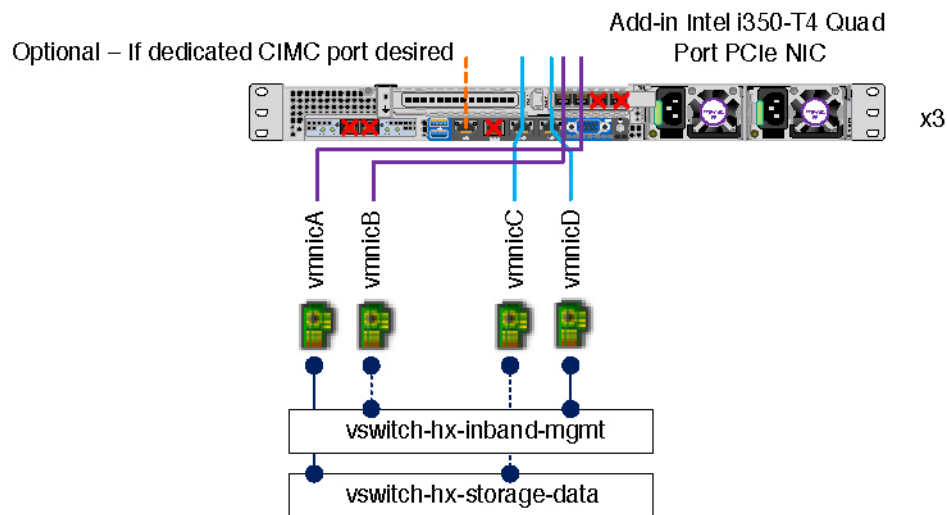
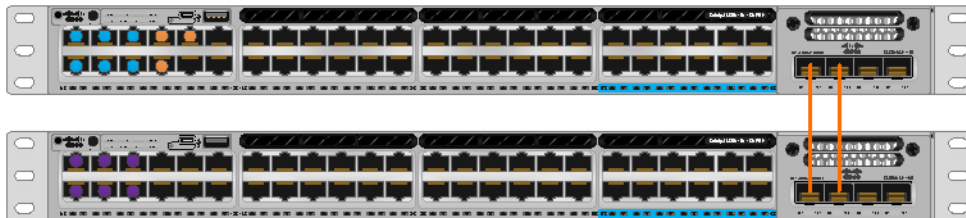
- 1 LOM and 1 PCIe port serve storage data and vMotion traffic in a redundant and load balanced configuration
- The Intel i350 quad port NIC (UCSC-PCIE-IRJ45) must be installed for this topology:
 - The NIC may be selected at ordering time and shipped preinstalled from the factory.
 - The NIC may also be field-installed if ordered separately. Either riser #1 or #2 may be used, although riser #1 is recommended.
- Only trunk ports are supported in the dual switch configuration.
- Spanning tree portfast trunk must be enabled for all network ports connected to HyperFlex servers.
 - Failure to configure portfast causes intermittent CIMC disconnects during ESXi bootup and longer than necessary network re-convergence during physical link failure.

Physical network topology guidance:



Warning

Proper cabling is important to ensure full network redundancy.



- Cable both integrated LOM ports to the same ToR switch.
- Cable any two out of four PCIe NIC ports to the same ToR switch. Do not connect more than two PCIe NIC ports prior to installation. Post cluster installation, you may freely use the remaining ports.

- Redundancy occurs at the vSwitch level and includes one uplink port from the onboard LOM and one uplink port from PCIe NIC for each vSwitch
- If desired, cable the dedicated CIMC port to the same switch or to an out-of-band management switch.
- Do not use the 10GE ports on the VIC.

Common Network Requirements

Before you begin installation, confirm that your environment meets the following specific software and hardware requirements.

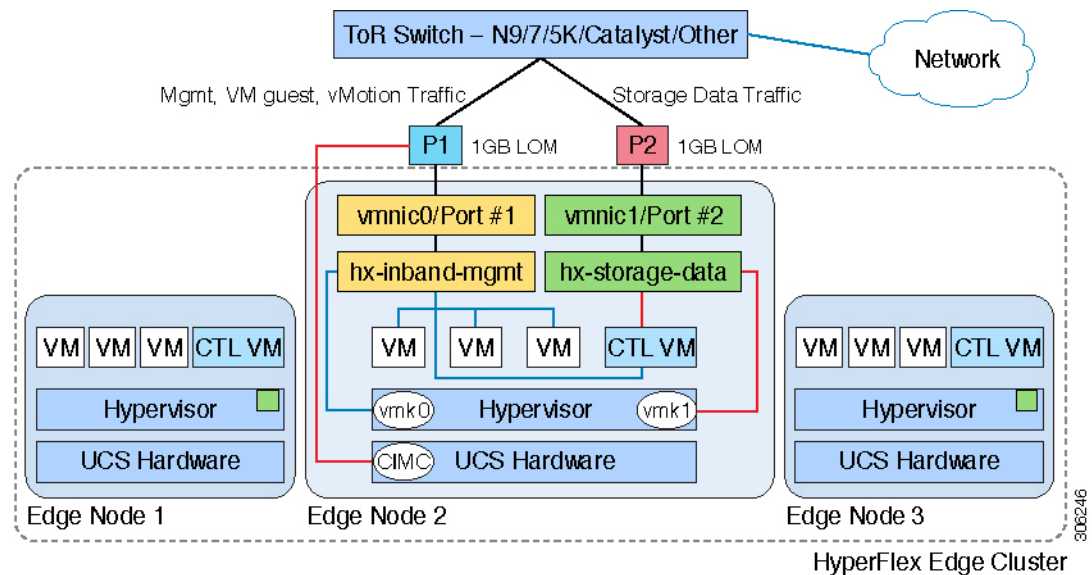


Attention

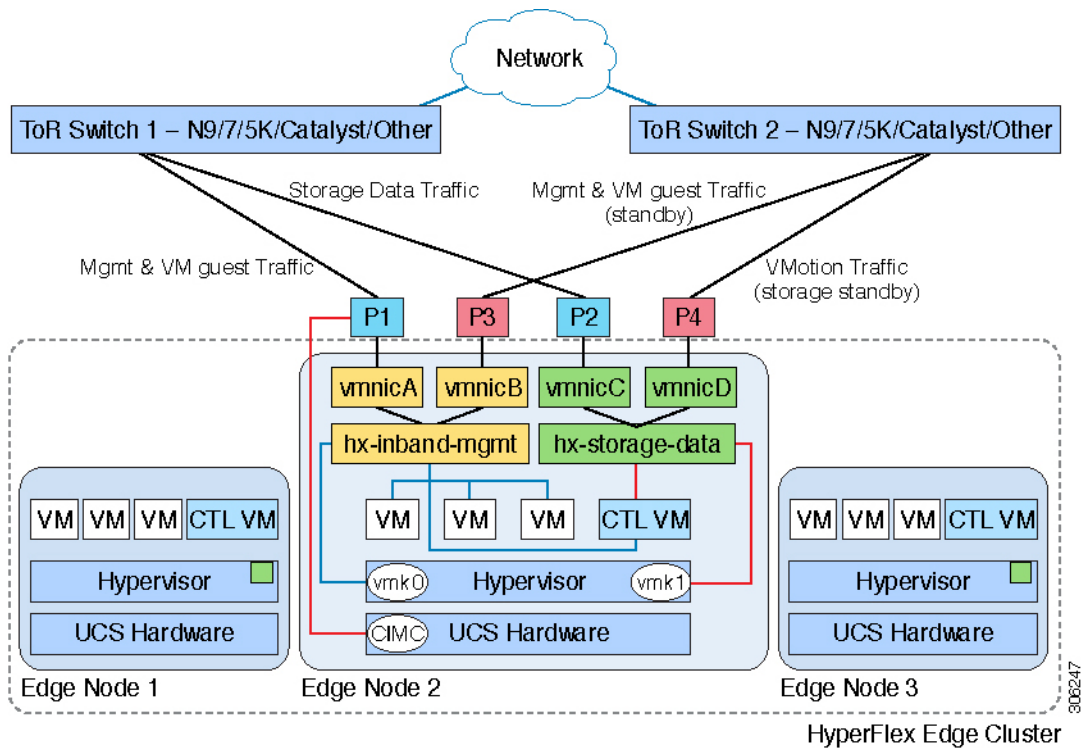
On HyperFlex M5 nodes, when using a 1GE topology manually configure the port speed to 1000/full on all switch ports. See the [Common Network Requirements, on page 9](#).

VLAN Requirements

Single Switch Network Topology



Dual Switch Network Topology



Network	VLAN ID	Description
Use a separate subnet and VLANs for each of the following networks:		
VLAN for VMware ESXi, and Cisco HyperFlex management		Used for management traffic among ESXi, HyperFlex, and VMware vCenter, and must be routable. Note This VLAN must have access to Intersight.
CIMC VLAN		Can be same or different from the Management VLAN. Note This VLAN must have access to Intersight.
VLAN for HX storage traffic		Used for storage traffic and requires only L2 connectivity.
VLAN for VMware vMotion		Used for vMotion VLAN, if applicable. Note Can be the same as the management VLAN but not recommended.

Network	VLAN ID	Description
VLAN(s) for VM network(s)		Used for VM/application network. Note Can be multiple VLANs separated by a VM portgroup in ESXi.

Inband versus Out-of-Band CIMC

This guides assume the use of inband CIMC using Shared LOM Ext mode. The result is CIMC management traffic multiplexed with vSphere traffic onto the LOM ports, reducing cabling, switchports, and additional configuration.

Customers may opt to use the dedicated CIMC management port for out-of-band use. Users should account for this third IGE port when planning their upstream switch configuration. Additionally, the user should set the CIMC to dedicated mode during CIMC configuration. Follow [Cisco UCS C-series documentation](#) to configure the CIMC in dedicated NIC mode. Under **NIC properties**, set the NIC mode to **dedicated** before saving the configuration.

In either case, CIMC must have network access to Intersight.

Supported vCenter Topologies

Use the following table to determine the topology supported for vCenter.

Topology	Description	Recommendation
Single vCenter	Virtual or physical vCenter that runs on an external server and is local to the site. A management rack mount server can be used for this purpose.	Highly recommended
Centralized vCenter	vCenter that manages multiple sites across a WAN.	Highly recommended
Nested vCenter	vCenter that runs within the cluster you plan to deploy.	Installation for a HyperFlex Edge cluster may be performed without a vCenter. Alternatively, you may deploy with an external vCenter and migrate it into the cluster. For the latest information, see the How to Deploy vCenter on the HX Data Platform tech note.

Customer Deployment Information

A typical three-node HyperFlex Edge deployment requires 13 IP addresses – 10 IP addresses for the management network and 3 IP addresses for the vMotion network.

CIMC Management IP Addresses

Server	CIMC Management IP Addresses
Server 1	
Server 2	
Server 3	
Subnet mask	
Gateway	
DNS Server	
NTP Server	
Note NTP configuration on CIMC is required for proper Intersight connectivity.	

Network IP Addresses

Note By default, the HX Installer automatically assigns IP addresses in the 169.254.1.X range, to the Hypervisor Data Network and the Storage Controller Data Network.



Note Spanning Tree portfast trunk (trunk ports) should be enabled for all network ports. Failure to configure portfast may cause intermittent disconnects during ESXi bootup and longer than necessary network re-convergence during physical link failure.

Management Network IP Addresses**(must be routable)**

Hypervisor Management Network	Storage Controller Management Network
Server 1:	Server 1:
Server 2:	Server 2:
Server 3:	Server 3:
Storage Cluster Management IP address	
Subnet mask	
Default gateway	

VMware vMotion Network IP Addresses

For vMotion services, you may configure a unique VMkernel port or, if necessary, reuse the vmk0 if you are using the management VLAN for vMotion (not recommended).

Server	vMotion Network IP Addresses (configured using the post_install script)
Server 1	
Server 2	
Server 3	
Subnet mask	
Gateway	

Port Requirements



Important

Ensure that the following port requirements are met in addition to the prerequisites listed for [Intersight Connectivity](#).

If your network is behind a firewall, in addition to the standard port requirements, VMware recommends ports for VMware ESXi and VMware vCenter.

- CIP-M is for the cluster management IP.
- SCVM is the management IP for the controller VM.
- ESXi is the management IP for the hypervisor.

The comprehensive list of ports required for component communication for the HyperFlex solution is located in Appendix A of the [HX Data Platform Security Hardening Guide](#)



Tip

If you do not have standard configurations and need different port settings, refer to [Table C-5 Port Literal Values](#) for customizing your environment.

Hypervisor Credentials

<i>root</i> username	root
<i>root</i> password	Cisco123 Important Deployments based on Cisco HX Data Platform Release, 3.0 and higher, require a new custom password if you have not changed the default factory password prior to starting installation.

VMware vCenter Configuration



Note HyperFlex communicates with vCenter through standard ports. Port 80 is used for reverse HTTP proxy and may be changed with TAC assistance. Port 443 is used for secure communication to the vCenter SDK and may not be changed.

vCenter admin username <i>username@domain</i>	
vCenter admin password	
vCenter data center name	
VMware vSphere compute cluster and storage cluster name	

Network Services



Note

- DNS and NTP servers should reside outside of the HX storage cluster.
- Use an internally-hosted NTP server to provide a reliable source for the time.
- All DNS servers should be pre-configured with forward (A) and reverse (PTR) DNS records for each ESXi host before starting deployment. When DNS is configured correctly in advance, the ESXi hosts are added to vCenter via FQDN rather than IP address.

Skipping this step will result in the hosts being added to the vCenter inventory via IP address and require users to change to FQDN using the following procedure: [Changing Node Identification Form in vCenter Cluster from IP to FQDN](#).

DNS Servers <i><Primary DNS Server IP address, Secondary DNS Server IP address, ... ></i>	
NTP servers <i><Primary NTP Server IP address, Secondary NTP Server IP address, ... ></i>	
Time zone <i>Example: US/Eastern, US/Pacific</i>	

Connected Services

Enable Connected Services (Recommended) <i>Yes or No required</i>	
Email for service request notifications <i>Example: name@company.com</i>	

Supported VMware vSphere Versions and Editions

Confirm that a compatible version of vSphere is preinstalled on all HyperFlex servers.

HyperFlex Version	VMware vSphere Versions	VMware vSphere Editions
4.0	6.0 U1b, 6.0 U2, 6.0 U2 patch 3, 6.0 U2 patch 4, 6.0 U3, 6.5 U1, 6.7 U2	Enterprise, Enterprise Plus, Standard, Essentials Plus, ROBO
3.5(x)		Enterprise, Enterprise Plus, Standard, Essentials Plus, ROBO
3.0	6.0 U3, 6.5 U1, 6.5 U2	Enterprise, Enterprise Plus, Standard, Essentials Plus, ROBO

Physical Requirements

HX220c nodes are 1 RU each. For a three-node cluster, 3 RU are required.

Reinstallation

To perform reinstallation of a HyperFlex Edge System, contact Cisco TAC.

HyperFlex Edge and Firmware Compatibility Matrix for 3.x Deployments

Cisco HX Data Platform, Release 3.x based Deployments

Confirm the component firmware on the server meets the minimum versions listed in the following tables.

**Important**

HyperFlex Edge does not support Cisco IMC versions 4.0(4a), 4.0(4b), 4.0(4c), 4.0(4d), and 4.0(4e).

Table 1: HX220c M4 / HXAF220c M4 Cluster

Component	Minimum Firmware Version - HXDP 3.x *(be sure to review important note(s) above)	Recommended Firmware Version - HXDP 3.x *(be sure to review important note(s) above)
Cisco Integrated Management Controller (CIMC)	3.0(3f)	4.0(2f)
Host Upgrade Utility (HUU) Download Link	3.0(3f) Download Software	4.0(2f) Download Software

Table 2: HX220c M5 / HXAF220c M5 Cluster

Component	Minimum Firmware Version - HXDP 3.x *(be sure to review important note(s) above)	Recommended Firmware Version - HXDP 3.x *(be sure to review important note(s) above)
Cisco Integrated Management Controller (CIMC)	3.1(2d)	4.1(2f)
Host Upgrade Utility (HUU) Download Link	3.1(2d) Download Software	4.1(2f) Download Software

Intersight Connectivity

Consider the following prerequisites pertaining to Intersight connectivity:

- Before installing the HX cluster on a set of HX servers, make sure that the device connector on the corresponding UCS Manager instance is properly configured to connect to Cisco Intersight and claimed.
- All device connectors must properly resolve `svc.ucs-connect.com` and allow outbound initiated HTTPS connections on port 443. The current version of the HX Installer supports the use of an HTTP proxy, except when the cluster is redeployed and is not new from the factory.
- All controller VM management interfaces must properly resolve `download.intersight.com` and allow outbound initiated HTTPS connections on port 443. The current version of HX Installer supports the use of an HTTP proxy if direct Internet connectivity is unavailable, except when the cluster is redeployed and is not new from the factory.
- The intended ESX server, HX Controller network, and vCenter host must be accessible through UCS Fabric Interconnect management interfaces.
- Starting with HXDP release 3.5(2a), the Intersight installer does not require a factory installed controller VM to be present on the HyperFlex servers.

In addition, on post-cluster deployment the new HX cluster is automatically claimed in Intersight for ongoing management.



CHAPTER 3

Installation

- [Installation Overview, on page 17](#)
- [Rack Cisco HyperFlex Nodes, on page 18](#)
- [Cisco Integrated Management Controller Configuration, on page 18](#)
- [Verifying Firmware Versions, on page 20](#)
- [Deploying Cisco HX Data Platform Installer, on page 21](#)
- [Configuring Your HyperFlex Cluster, on page 21](#)
- [Verifying Cisco HX Data Platform Software Installation, on page 27](#)
- [Cisco Intersight HX Installer for HyperFlex Edge, on page 27](#)

Installation Overview

Follow this workflow during installation:

Step	Description	Reference
1	Read the system requirements and complete the preinstall worksheet sections there.	<ul style="list-style-type: none">• Single Switch Configuration, on page 3 or Dual Switch Configuration, on page 6• Common Network Requirements, on page 9
2	Complete the installation prerequisites.	<ul style="list-style-type: none">• Rack Cisco HyperFlex Nodes, on page 18• Configure networking for Cisco Integrated Management Controller (CIMC). See Configuring CIMC: Static Assignment, on page 18• Verify firmware versions. See Verifying Firmware Versions, on page 20

Step	Description	Reference
3	Deploy Cisco HyperFlex storage cluster.	<ul style="list-style-type: none"> • Download and deploy Cisco HX Data Platform Installer. See Deploying Cisco HX Data Platform Installer, on page 21 • Launch the Cisco HX Data Platform Installer, and create your HyperFlex storage cluster. See Configuring Your HyperFlex Cluster, on page 21 • Confirm Cisco HX Data Platform software installation in the vCenter Server. See Verifying Cisco HX Data Platform Software Installation, on page 27

Rack Cisco HyperFlex Nodes

For details on installation of Cisco HX220c M5 HyperFlex Nodes, see [Cisco HX220c M5 HyperFlex Node Installation Guide](#).



Important

You can use a console dongle to connect the VGA monitor and keyboard for CIMC configuration. You can also directly connect to the VGA and USB ports on the rear of the server. Alternatively, you can perform a lights-out configuration of CIMC if a DHCP server is available in the network.

Cisco Integrated Management Controller Configuration

Choose one method for CIMC network configuration: static assignment or DHCP assignment.

Configuring CIMC: Static Assignment

To configure Cisco Integrated Management Controller (CIMC), you must enable CIMC standalone mode, configure the CIMC password and settings, and configure a static IP address manually using a KVM. This requires physical access to each server with a monitor and keyboard. Each server must be configured one at a time.

Customers may opt to use the dedicated CIMC management port for out-of-band use. Users should account for this third 1GE port when planning their upstream switch configuration. Additionally, the user should set the CIMC to dedicated mode during CIMC configuration. Follow [Cisco UCS C-series documentation](#) to configure the CIMC in dedicated NIC mode. Under **NIC properties**, set the NIC mode to **dedicated** before saving the configuration.

Before you begin

- Ensure that all Ethernet cables are connected as described in the [Preinstallation Checklist, on page 3](#) section.

- Attach the VGA dongle to the server and connect a monitor and USB keyboard.

-
- Step 1** Power on the server, and wait for the screen with the Cisco logo to display.
- Step 2** When prompted for boot options, press **F8** to enter the **Cisco IMC Configuration** utility.
- Step 3** In **CIMC User Details**, enter **password** for the **current CIMC password**, enter your **new CIMC password** twice, and press **Enter** to save you new password.
- Important** Systems ship with a default password of *password* that must be changed during installation. You cannot continue installation unless you specify a new user supplied password.
- Step 4** For **IP (Basic)**, check **IPv4**, uncheck **DHCP enabled**, and enter values for **CIMC IP**, **Prefix/Subnet** mask, and **Gateway**.
- Step 5** For **VLAN (Advanced)**, check **VLAN enabled**, and:
- If you are using trunk ports, set the appropriate **VLAN ID**.
 - If you are using access ports, leave this field blank.
- Step 6** Leave the rest of the settings as default, press **F10** to save your configuration, and press **ESC** to exit the utility.
- Step 7** In a web browser, navigate directly to the CIMC page at **https://CIMC IP address**.
- Step 8** Enter the username **admin** and your new CIMC password, and click **Log In**.
- Step 9** Manually set the power policy to match the desired operation from **Server > Power Policies**.
- Servers default to the Power Off power-restore policy set at the factory.
-

What to do next

You can use the virtual KVM console or continue to use the physical KVM. The SD cards have ESXi preinstalled from the factory and boot automatically during installation.

Configuring CIMC: DHCP Assignment

To configure Cisco Integrated Management Controller (CIMC), you must enable CIMC standalone mode, configure the CIMC password and settings, and configure a dynamic IP address obtained through DHCP. This requires more network setup but eases configuration by enabling a lights-out setup of HyperFlex Edge nodes. All servers lease addresses automatically and in parallel, reducing deployment time.

Before you begin

- Ensure that all Ethernet cables are connected as described in the [Preinstallation Checklist, on page 3](#) section.
- Ensure the DHCP server is properly configured and running with a valid scope.
- Ensure the DHCP server is directly listening on the management VLAN or you have an IP helper configured on your switch(es).
- Decide on inband versus out-of-band CIMC:

- If using inband CIMC, configure the native VLAN for all HyperFlex Edge switch ports to match the correct DHCP VLAN. This is the only way to ensure that the CIMC can lease an address automatically.
- If using out-of-band CIMC, configure the dedicated switch port for access mode on the DHCP VLAN.

-
- Step 1** Connect power cables.
- Step 2** Access the DHCP logs or lease table to determine the CIMC addresses obtained
- Step 3** Search the hostnames for **C220-*<S/N>*** to find your HyperFlex servers, and make note of the addresses for required inputs into the HX Data Platform Installer.
-

What to do next

When using DHCP, you must manually set a user defined CIMC password before beginning HyperFlex Data Platform installation. Use either the web UI or a CLI session to set a new password. The default password of **password** must be changed or installation fails.

Verifying Firmware Versions

You need to view current BIOS, CIMC, SAS HBA, and drive firmware versions, and verify that those versions match data in the Release Notes.

-
- Step 1** In your browser, log in to the CIMC web UI by navigating to **https://*<CIMC IP>***.
- Step 2** In the Navigation pane, click **Server**.
- Step 3** On the **Server** page, click **Summary**.
- Step 4** In the **Cisco Integrated Management Controller (CIMC) Information** section of the **Server Summary** page, locate and make a note of the **BIOS Version** and **CIMC Firmware Version**.
- Step 5** In CIMC, navigate to **Inventory > PCIe Adapters**, and locate and make a note of the **SAS HBA Version**.
- Step 6** In CIMC, navigate to **Inventory > Storage Adapters**.
- Step 7** Depending on which server type you are using, navigate to one of the following:
- For M4, **UCSC-SAS12GHBA > Details > Physical Drive Info**, and make a note of the drive type, manufacturer, and firmware version.
 - For M5, **UCSC-SAS-M5 > Details > Physical Drive Info**, and make a note of the drive type, manufacturer, and firmware version.
- Step 8** Compare the current BIOS, CIMC, SAS HBA, and drive firmware versions with the versions listed in the Release Notes.
- Step 9** If the minimum versions are not met, use the Host Update Utility (HUU) Download Links in the compatibility matrix to upgrade the firmware versions running on the system, including Cisco Virtual Interface Cards (VIC), PCI Adapter, RAID controllers, and drive (HDD/SSD) firmware. You can find current and previous releases of the Cisco HUU User Guide at this location: <http://www.cisco.com/c/en/us/support/servers-unified-computing/ucs-c-series-rack-servers/products-user-guide-list.html>.
-

Deploying Cisco HX Data Platform Installer

HX Data Platform Installer can be deployed on an ESXi server, as well as a VMware Workstation, VMware Fusion, or Virtual Box. The HyperFlex software is distributed as a deployable virtual machine, contained in an Open Virtual Appliance (OVA) file format. Use the following procedure to deploy HX Data Platform Installer using a VMware vSphere (thick) Client.

-
- Step 1** Download the HX Data Platform Installer OVA from [Cisco.com](https://www.cisco.com), and save the package locally.
Verify the downloaded version matches the recommended version for your deployment.
- Step 2** Log in to vCenter using the vSphere client.
- Step 3** Select **File > Deploy OVF Template**.
- Step 4** In the **Deploy OVF Template** wizard, on the **Source** page, specify the source location, and click **Next**.
- Step 5** On the **OVF Template Details** page, view the information, and click **Next**.
- Step 6** (Optional) On the **Name and Location** page, edit the name and location for the virtual appliance, and click **Next**.
- Step 7** On the **Host/Cluster** page, select the host or cluster on which you want to deploy, and click **Next**.
- Step 8** On the **Resource Pool** page, select the resource pool where you want to run the OVF template, and click **Next**.
- Step 9** On the **Storage** page, select a datastore to store the deployed OVF template, and click **Next**.
- Step 10** On the **Disk Format** page, select the disk format to store the virtual machine virtual disks, and click **Next**.
- Step 11** On the **Network Mapping** page, for each network specified in the OVF template, right-click the **Destination Network** column to select a network in your infrastructure, and click **Next**.
- Step 12** Provide the OVF properties for the installer VM, namely: hostname, default gateway, DNS server, IP address, and subnet mask.

Alternatively, leave all of the OVF properties blank for a DHCP assigned address.
- Step 13** On the **Ready to Complete** page, select **Power On After Deployment**, and click **Finish**.
-

Configuring Your HyperFlex Cluster

-
- Step 1** In your web browser, enter the IP address of the installer VM, and click **Accept** or **Continue** to bypass any SSL certificate errors.
- Step 2** Verify the HyperFlex installer **Build ID** in the lower right corner of the login screen.
- Step 3** Log in to Cisco HX Data Platform Installer using username **root** and password **Cisco123**.
Important Systems ship with a default password of *Cisco123* that must be changed during installation. The HyperFlex on-premise installer requires changing the root password as part of deployment. You cannot continue installation unless you specify a new password. Use the new password at this point in the configuration procedure.
- Step 4** Read the End User Licensing Agreement, check **I accept the terms and conditions**, and click **Login**.
- Step 5** On the **Workflow** page, click **Cluster Creation with HyperFlex Edge**.

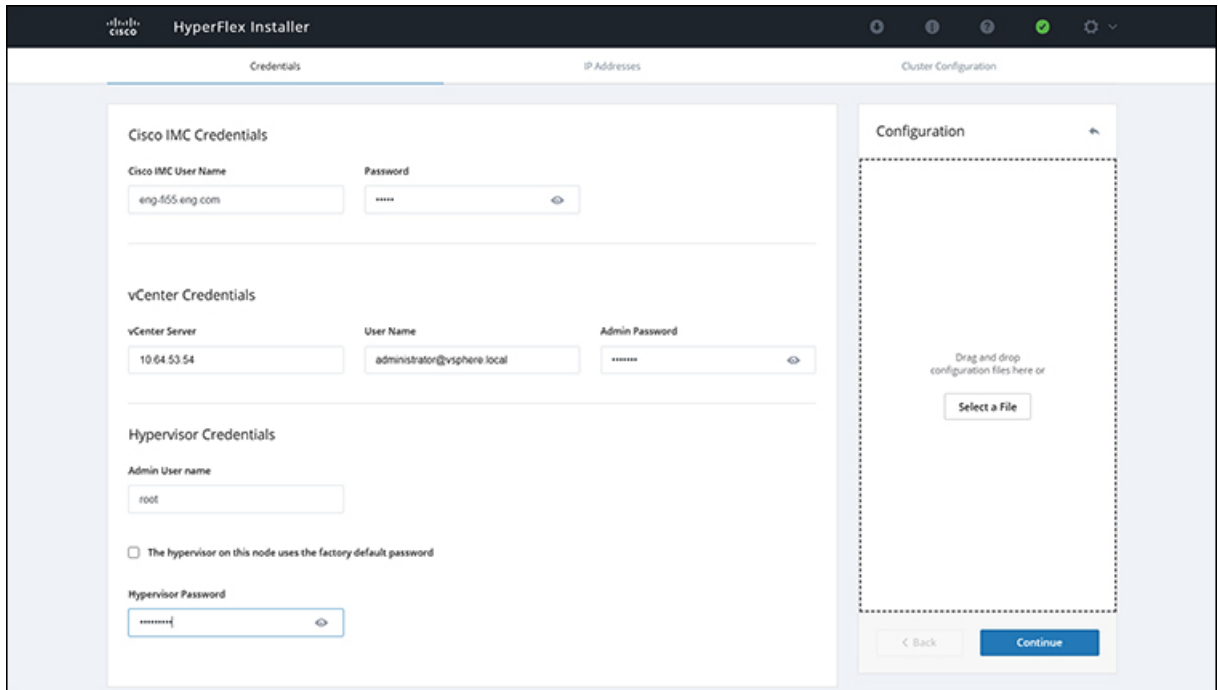
Step 6 To perform cluster creation, you can import a *JSON configuration* file with the required configuration data. The following two steps are optional if importing a JSON file, otherwise you can input data into the required fields manually.

- Note** For a first-time installation, contact your Cisco representative to procure the factory preinstallation JSON file.
- a. Click **Select a file** and choose your *JSON file* to load the configuration. Select **Use Configuration**.
 - b. An **Overwrite Imported Values** dialog box displays if your imported values for Cisco UCS Manager are different. Select **Use Discovered Values**.

Step 7 On the **Credentials** page, complete the following fields, and click **Continue**.

Name	Description
Cisco IMC Credentials	
Cisco IMC User Name	Cisco IMC username. By default, the user name is admin .
Password	CIMC password. By default, the password is password .
vCenter Credentials	
vCenter Server	FQDN or IP address of the vCenter server. You must use an account with vCenter root-level admin permissions.
User Name	Administrator username.
Admin Password	Administrator password.
Hypervisor Credentials	
Admin User Name	Administrator username. By default, the username is root .
Hypervisor Password	Default password is Cisco123. Important Systems ship with a default password of <i>Cisco123</i> that must be changed during installation. You cannot continue installation unless you specify a new user supplied password.

Use the following screenshot as a reference to complete the fields in this page.



Step 8 On the **IP Addresses** page, enter the assigned addresses for each server.

Name	Description
Cisco IMC	IP Address of Cisco IMC
Hypervisor	Management IP for Hypervisor
Storage Controller	Management IP for Storage Controller
Cluster IP Address	Cluster management IP address
Subnet mask	Subnet mask for cluster management
Gateway	Gateway IP address for cluster management IP

Use the following screenshot as a reference to complete the fields in this page.

Step 9 On the **Cluster Configuration** page, complete the following fields, and click **Continue**.

Note Complete all the fields using your pre-install worksheet.

Name	Description
Cisco HX Cluster	
Cluster Name	User-supplied name for the HyperFlex storage cluster.
Replication Factor	
Controller VM	
Create Admin Password	There is no default password for the Controller VM. User needs to set this field
Confirm Admin Password	Confirm the Administrator password.
vCenter Configuration	
vCenter Datacenter Name	The name of the vCenter datacenter where the HyperFlex hosts were added.
vCenter Cluster Name	The name of the vCenter cluster where the HyperFlex hosts were added.
System Services	
DNS Server(s)	A comma-separated list of IP addresses for each DNS Server.

Name	Description
NTP Server(s)	A comma-separated list of IP addresses for each NTP Server. Important A highly reliable NTP server is required.
Time Zone	The local time zone for the controller VM.
Connected Services	
Enable Connected Services (Recommended)	Check to Enable Connected Services. Note We highly recommend enabling Connected Services to enable sending email alerts to Cisco TAC.
Send service ticket notifications to: <i>Example:</i> <i>admin@cisco.com</i>	Email address to receive service request notifications.
Advanced Networking	
Management VLAN Tag Data VLAN Tag	Enter the correct VLAN tags if you are using trunk ports. The VLAN tags must be different when using trunk mode. Enter 0 for both VLAN tags if you are using access ports. Note Do not enter 0 if you are using trunk ports.
Management vSwitch Data vSwitch	Do not change the auto-populated vSwitch name.
Advanced Configuration	
Enable Jumbo Frames on Data Network	Do not check to ensure HyperFlex Edge deployments use regularly-sized packets. You may optionally enable jumbo frames for 10/25GE deployments depending on your network configuration. For ease of deployment, it is recommended to uncheck this option.
Clean up disk partitions	Check to remove all existing data and partitions from every node in the HX storage cluster. For example, if this is not the first time installing the software on the cluster.
Optimize for VDi only deployment	Check to optimize VDI deployments. By default HyperFlex is performance optimized for Virtual Server Infrastructure (VSI). Check this box to tune the performance parameters for VDI deployments. This option has no affect on all-flash HX models and only needs to be enabled for hybrid HX clusters. If you are running mixed VDI and VSI workloads, do not select this option.
vCenter Single-Sign-On Server	Fill in this field only if instructed by Cisco TAC.

Use the following screenshot as a reference to complete the fields in this page.

The screenshot displays the HyperFlex Installer web interface, specifically the 'Cluster Configuration' page. The interface is organized into several sections:

- Cisco HX Cluster:** Includes 'Cluster Name' (EDGE_CLUSTER) and 'Replication Factor' (2).
- Controller VM:** Includes 'Create Admin Password' and 'Confirm Admin Password' fields.
- vCenter Configuration:** Includes 'vCenter Datacenter Name' (datacenter) and 'vCenter Cluster Name' (cluster).
- System Services:** Includes 'DNS Server(s)' (10.64.48.21), 'NTP Server(s)' (10.64.1.48), 'DNS Domain Name', and 'Time Zone' (UTC+05:30 Chennal, Sri Jayawardenepura).
- Connected Services:** Includes 'Enable Connected Services (Recommended)' (checked) and 'Send service ticket notifications to' (admin@cisco.com).
- Advanced Networking:** Includes 'Management VLAN Tag' (10), 'Management vSwitch' (vswitch-hx-inband-mgmt), 'Data VLAN Tag' (11), and 'Data vSwitch' (vswitch-hx-storage-data).
- Advanced Configuration:** Includes 'Jumbo Frames' (checked), 'Disk Partitions' (checked), 'Virtual Desktop (VDI)' (checked), and 'vCenter Single-Sign-On Server' (ex: https://<address>-7444/sts/STSService).

The right-hand sidebar provides a summary of the configuration:

- Credentials:** vCenter Server (10.64.53.54), User Name (administrator@vsphere.local), Cisco IMC User Name (eng-f55.eng.com), Admin User name (root).
- IP Addresses:** Cluster Name (EDGE_CLUSTER), Management Cluster (10.10.10.40), Management Subnet Mask (255.0.0.0), Management Gateway (10.10.10.1).
- Server 1:** Management Cisco IMC (10.10.10.10), Management Hypervisor (10.10.10.20), Management Storage Controller (10.10.10.30).
- Server 2:** Management Cisco IMC (10.10.10.11).

Navigation buttons for '< Back' and 'Start' are located at the bottom of the sidebar.

Step 10 After deployment finishes, the **Summary Deployment** page displays a summary of the deployment details.

What to do next

Confirm HX Data Platform Plug-in installation. See [Verifying Cisco HX Data Platform Software Installation, on page 27](#)

Verifying Cisco HX Data Platform Software Installation

Step 1 Launch **vSphere Web Client**, and log in to the vCenter Server as an administrator.

Step 2 Under **vCenter Inventory Lists**, verify that **Cisco HX Data Platform** displays.

If the entry for Cisco HX Data Platform does not appear, log out of vCenter, close the browser, and log back in. In most cases, the issue is resolved by this action.

If logging out of vCenter does not fix the issue, you may have to restart the vSphere Web Client. SSH to the VCSA and run `service vsphere-client restart`. For a Windows vCenter, restart VMware vSphere Web Client in the services page in mmc.

Step 3 Ensure that your new cluster is online and registered.

Cisco Intersight HX Installer for HyperFlex Edge

Intersight HX installer rapidly deploys HyperFlex Edge clusters. The installer constructs a pre-configuration definition of your cluster, called an HX Cluster Profile. This definition is a logical representation of the HX nodes in your HX Edge cluster. Each HX node provisioned in Cisco Intersight is specified in a HX Cluster profile.

Refer to the [Cisco HyperFlex Installation Guide for Cisco Intersight](#) for detailed deployment instructions.



CHAPTER 4

Post Installation Tasks

- [Post Installation Tasks Summary, on page 29](#)

Post Installation Tasks Summary

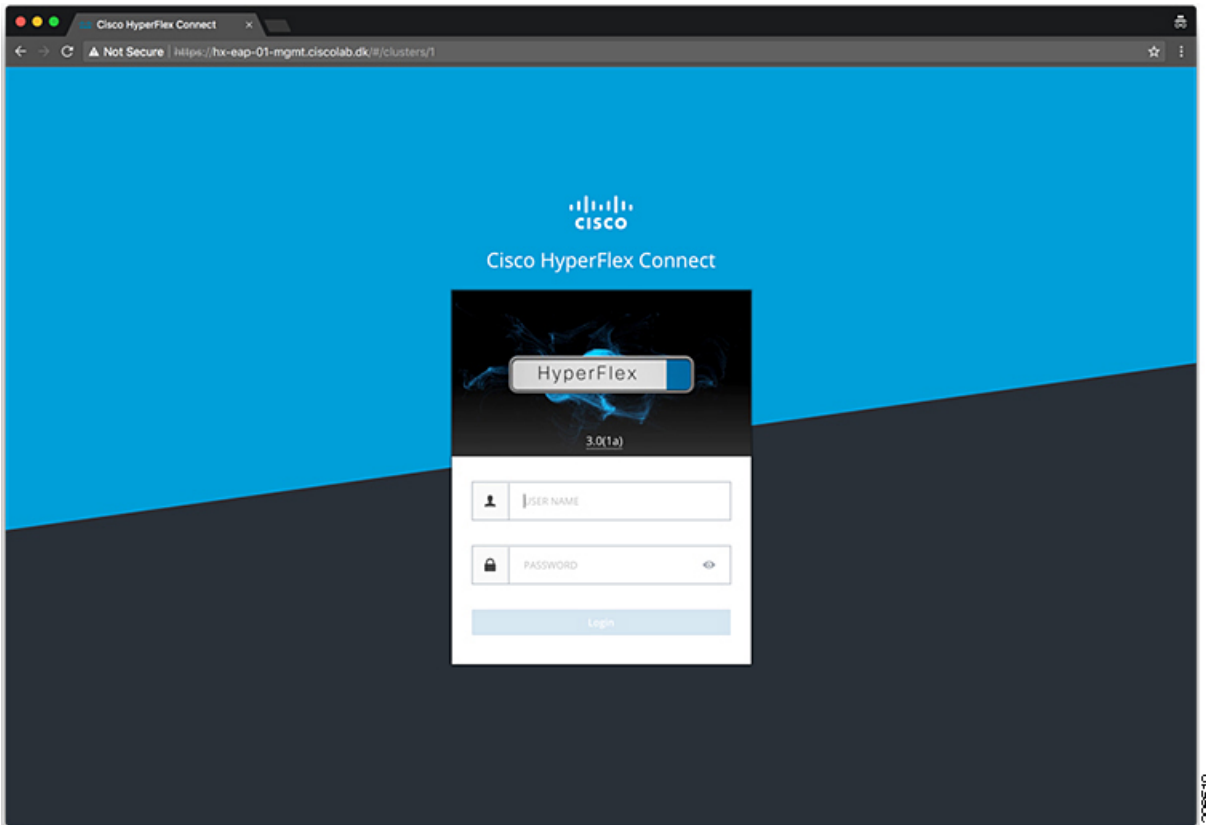
After successful cluster configuration, perform the following additional post installation tasks to ensure that the cluster is ready to serve VMs.

Task	Reference
Create the First Datastore	Create the First Datastore, on page 29
Assign a static IP address for Live Migration and VM Network	Configuring a Static IP Address for Live Migration and VM Network, on page 31
(Optional) Constrained Delegation	(Optional) Post Installation Constrained Delegation, on page 32
Configure Local Default Paths	Configure Local Default Paths, on page 33
Configure File Share Witness	Configuring a File Share Witness, on page 34
Checking the Windows Version on the Hyper-V Host	Checking the Windows Version on the Hyper-V Host, on page 40
Deploying VMs on a Hyper-V cluster	Deploying VMs on a Hyper-V cluster, on page 40
Configuring HyperFlex Share to SCVMM	Configuring HyperFlex Share to SCVMM, on page 46
Re-enabling Windows Defender	Re-enabling Windows Defender, on page 48

Create the First Datastore

Before you begin using the cluster, you must create a datastore. The datastore can be created in HX Connect UI.

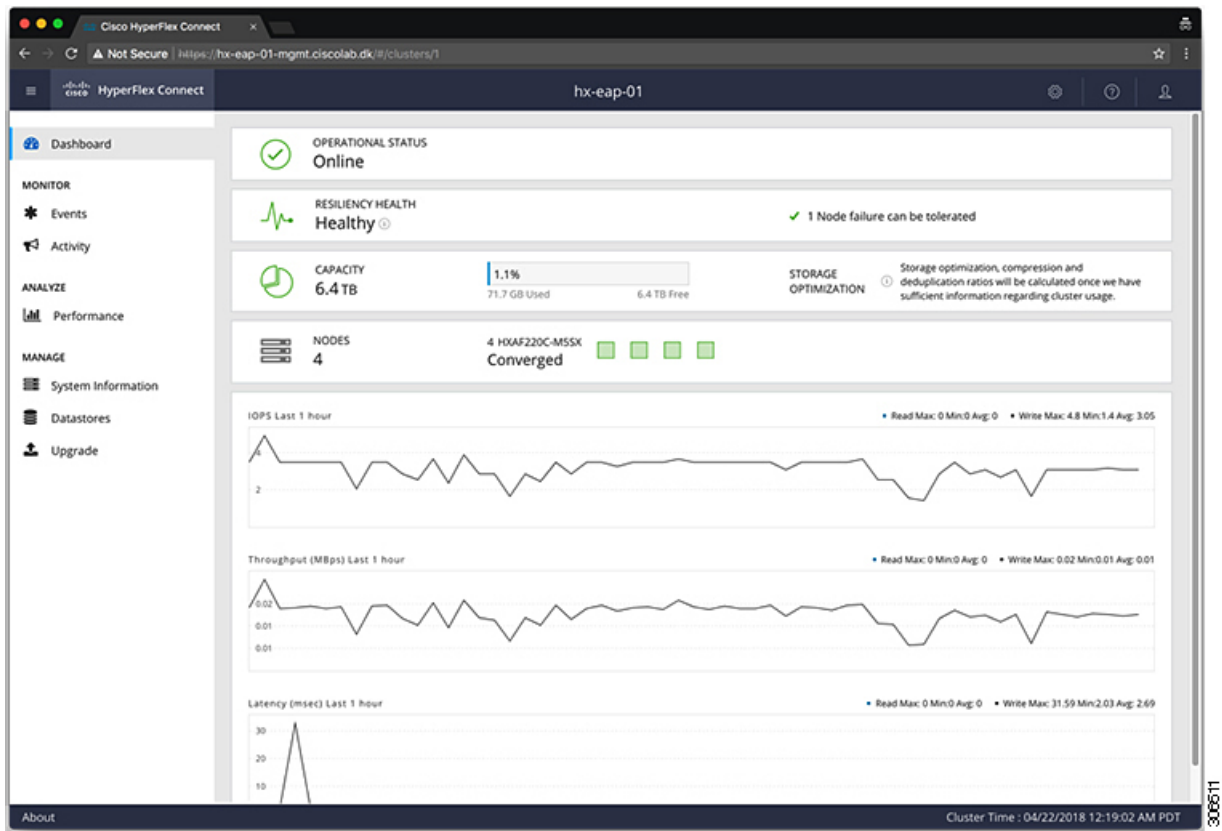
Step 1 Launch HX Connect UI from a browser of your choice from *https://Cluster_IP/* or *https://FQDN*.



Step 2 Log in with the following credentials:

- **Username**—**hxadmin**
- **Password**—Use the password set during cluster installation.

Step 3 In the Navigation pane, select **Datastores**.



Step 4 In the Work pane, click **Create Datastore**.

Step 5 In the **Create Datastore** dialog box, complete the following fields:

Field	Description
Datastore Name	Enter a name for the datastore. Cisco recommends that you use all lower case characters for the datastore name.
Size	Select the size for the datastore.
Block Size	Select the block size for the datastore.

Note Cisco recommends 8K block size and as few datastores as possible to ensure the best performance.

Configuring a Static IP Address for Live Migration and VM Network

Log in to each Hyper-V node and execute the following commands in Power Shell to assign a static IP address for Live Migration and VM Network.

#	Command	Purpose
1	<code>New-NetIPAddress -ifAlias "vSwitch-hx-livemigration" -IPAddress 192.168.73.21 -PrefixLength 24</code>	Assigns a static IP address to the Live Migration network.
2	<code>New-NetIPAddress -ifAlias "vswitch-hx-vm-network" -IPAddress 192.168.74.21 -PrefixLength 24</code>	Assigns a static IP address to the VM network.

(Optional) Post Installation Constrained Delegation



Attention

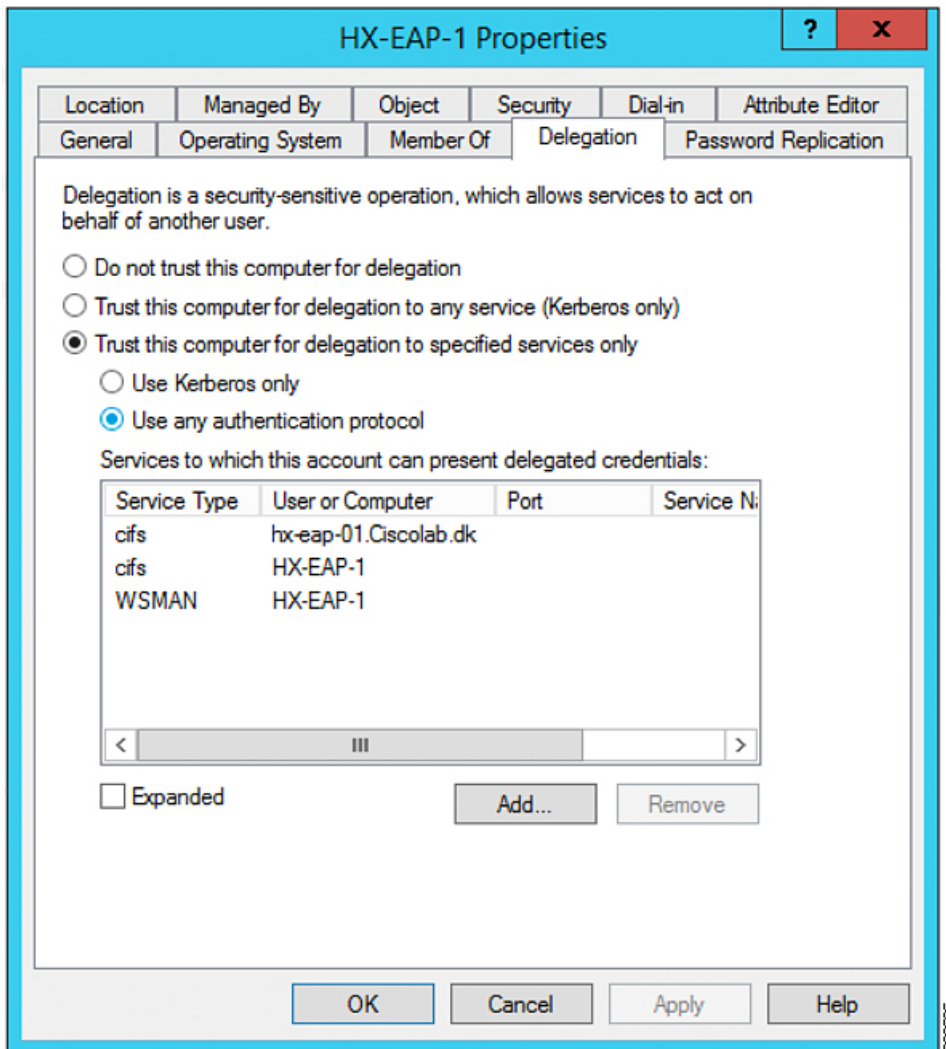
This step must be performed only if Constrained Delegation was not configured during initial installation. It is recommended that you perform this procedure using the HX Installer and not as part of post-installation.

Constrained Delegation gives granular control over impersonation. When the remote management requests are made to the Hyper-V hosts, it needs to make those requests to the storage on behalf of the caller. This is allowed if that host is trusted for delegation for the CIFS service principal of HX Storage.

Constrained Delegation requires that the option for the security setting **User Account Control: Behavior of the elevation prompt for Administrators in Admin Approval Mode** is set to **Elevate without Prompting**. This will prevent the global AD policy from overriding policy on HX OU.

Perform the following procedure *on each Hyper-V host in the HX Cluster* to configure using **Windows Active Directory Users and Computers**.

-
- Step 1** Click **Start**, click **Administrative Tools**, and then click **Active Directory Users and Computers**.
 - Step 2** Expand domain, and then expand the Computers folder.
 - Step 3** In the right pane, right-click on the computer name (for example, HX-Properties), and then click **Properties**.
 - Step 4** Click on the **Delegation** tab.
 - Step 5** Select **Trust this computer for delegation to specified services only**.
 - Step 6** Ensure that **Use any authentication protocol** is selected.
 - Step 7** Click **Add**. In the **Add Services** dialog box, click **Users or Computers**, and then browse or type the name of the Service Type (such as CIFS). Click OK. The following illustration can be used as an example.



Step 8 Repeat these steps for all nodes.

Configure Local Default Paths

Configure the default local path for the VMs to ensure that they will be on the HX cluster datastore.

Run the following commands in PowerShell:

```
$Creds = Get-Credential -Message "User Credentials" -UserName <<current logon username>>
$hosts = ("hostname1","hostname2","hostname3","hostname4")
Invoke-Command -ComputerName $hosts -Credential $Creds -ScriptBlock {Set-VMHost
-VirtualHardDiskPath
"\HX-EAP-01.ciscolab.dk\DS1_8K" -VirtualMachinePath "\HX-EAP-01.ciscolab.dk\DS1_8K"}
```



Note The username should either be a Domain admin account or the HX service account. The local Administrator on the Hyper-V host will not work.



Note Remember to change the variables to suit your environment.

Configuring a File Share Witness

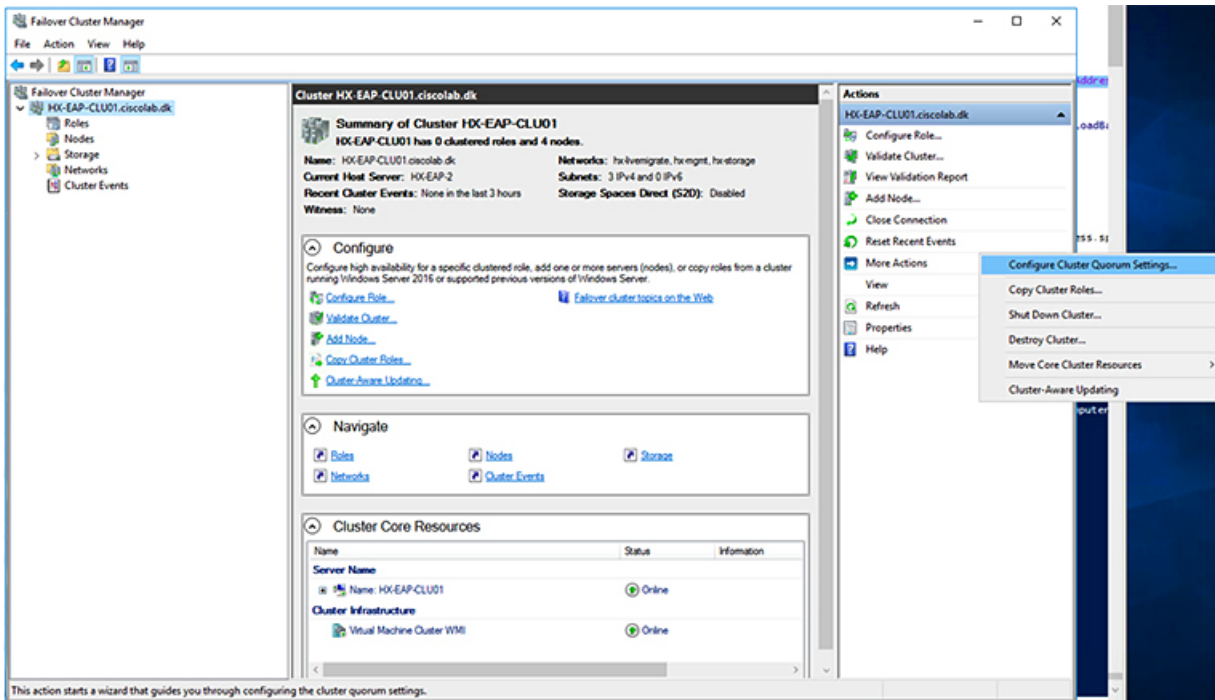
As a Microsoft best practice, ensure that you configure a Quorum witness datastore. Use the following procedure to configure a File Share Witness using **Failover Cluster Manager (FCM)**. A File Share Witness ensures high availability of the failover cluster when nodes on the network fail. Specifically, a File Share Witness is needed to maintain a failover cluster quorum, which is designed to prevent split-brain scenarios that may happen when a partition in the network and subsets of nodes cannot communicate with each other. For more information, see "[Understanding cluster and pool quorum](#)".



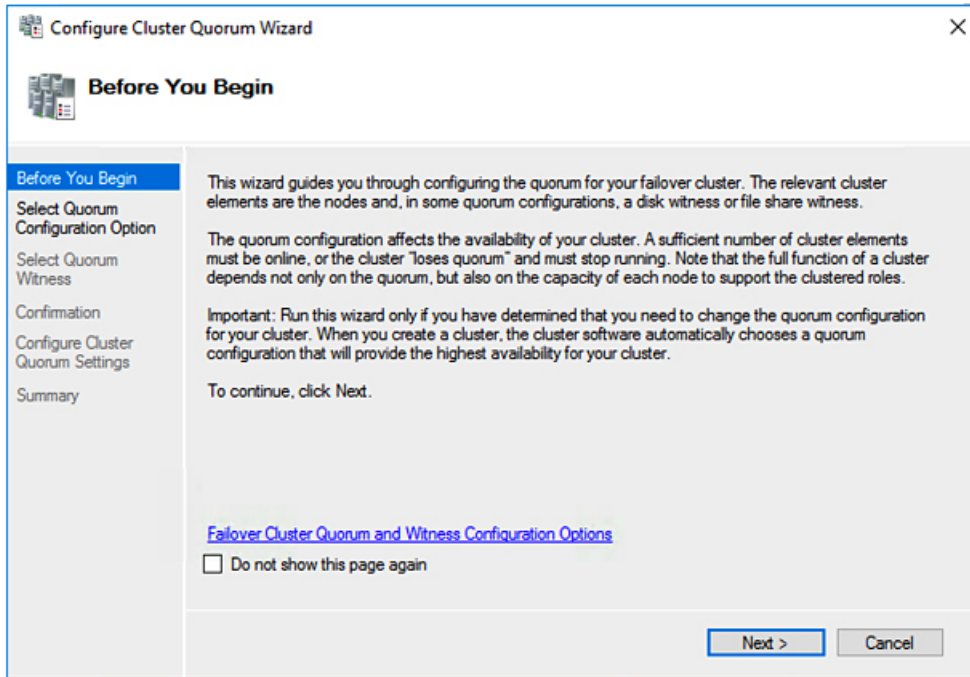
Note In an HX cluster, the storage is designed to be highly available and no host should lose access to the storage. In the event that one host does stop writing to the datastore, Microsoft's storage resiliency behavior kicks in. The host repeatedly retries to establish a connection with the storage for 30 mins by default. During this time, the user VMs may be paused. If it can not connect after 30 mins, the VM moves to a 'stopped' state.

Step 1 Launch FCM.

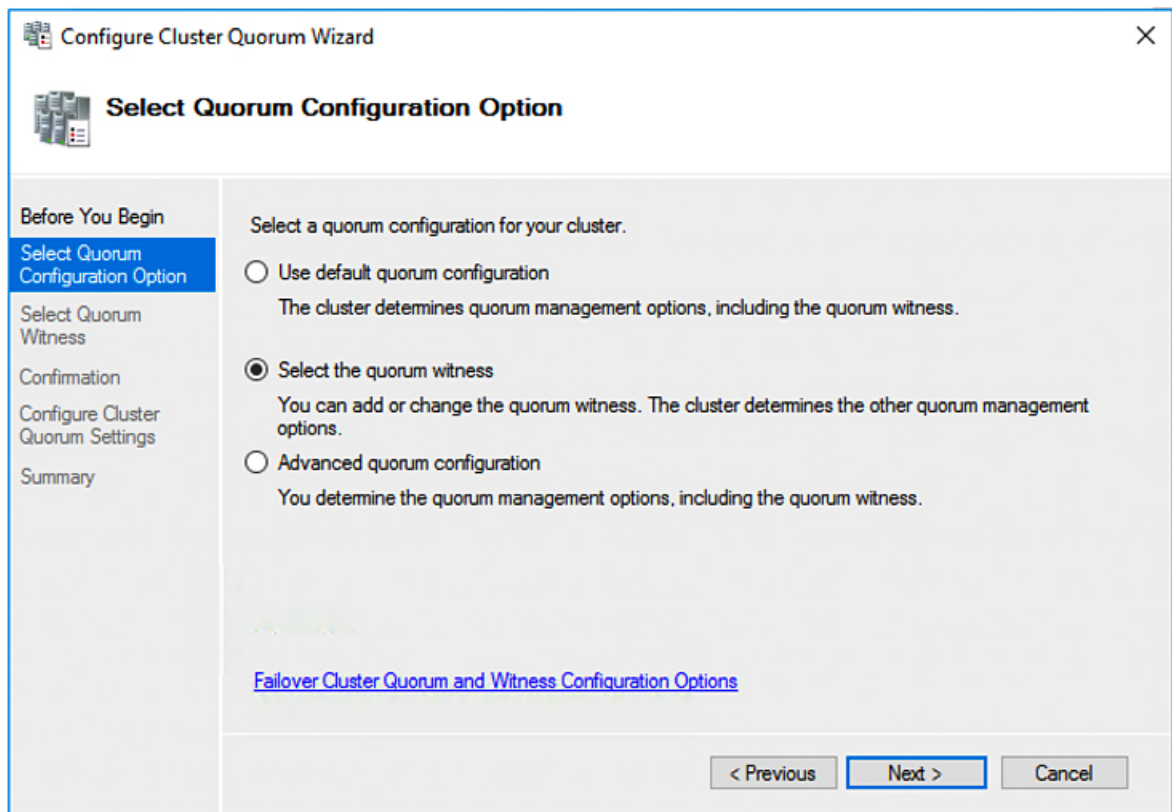
Step 2 In the navigation pane, select your cluster. Then, in the **Actions** pane, select **More Actions > Configure Cluster Quorum Settings...**



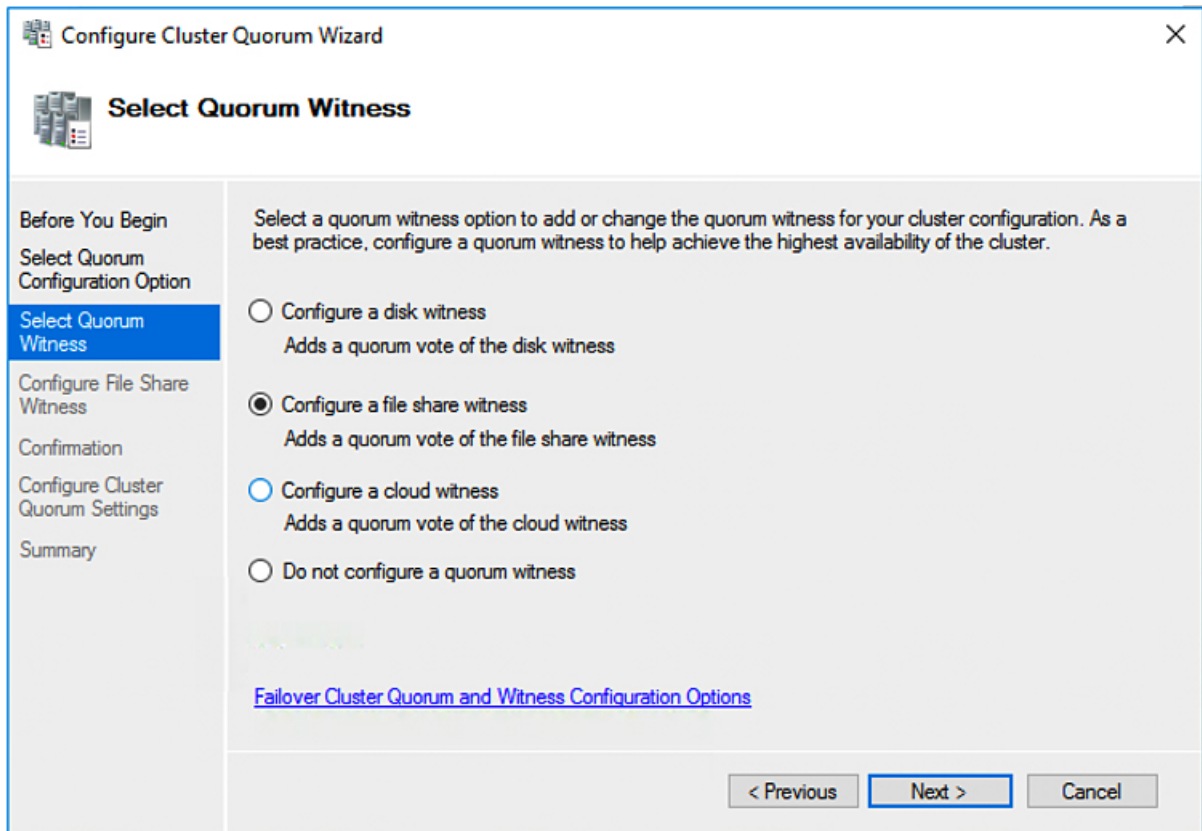
Step 3 The **Configure Cluster Quorum** wizard is launched. Click **Next**.



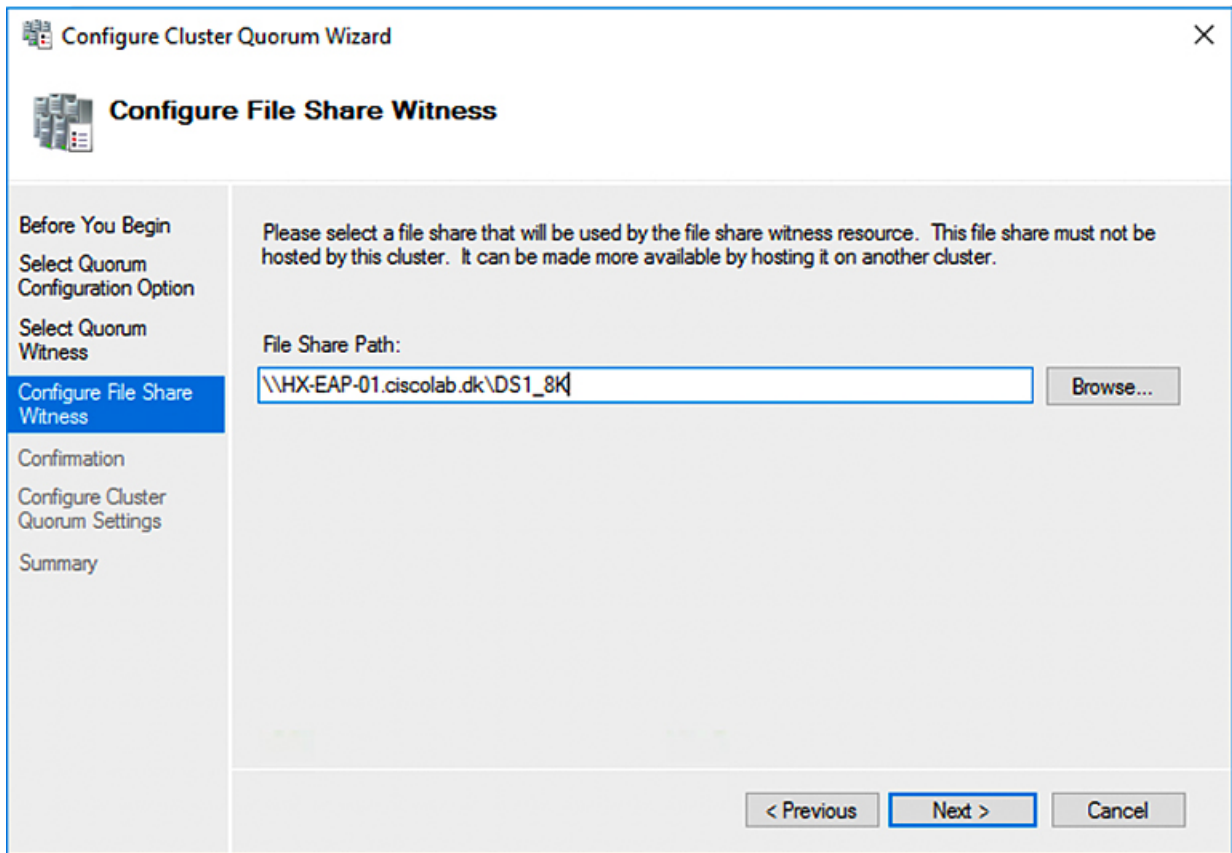
Step 4 In the **Select Quorum Configuration Option** screen, choose **Select the quorum witness**. Click **Next**.



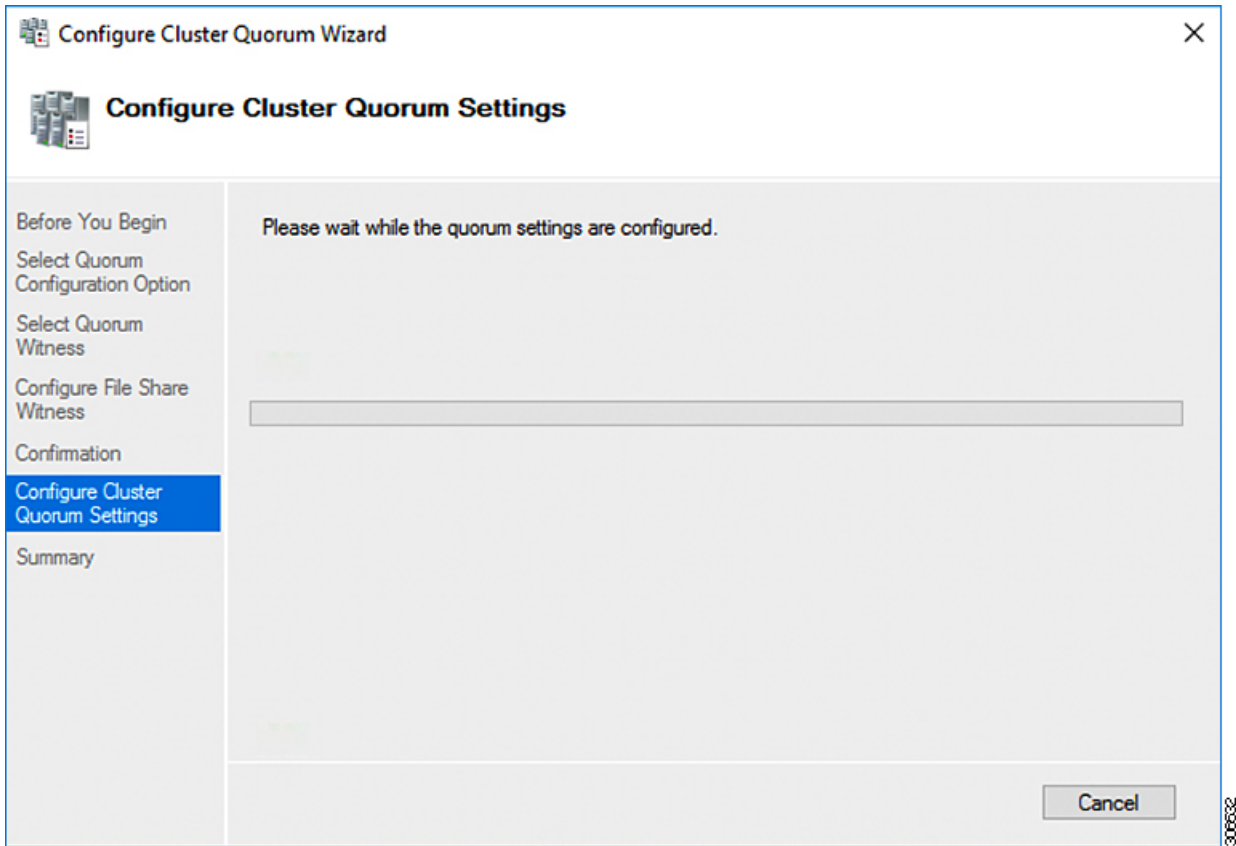
Step 5 In the **Select Quorum Witness** screen, choose **Configure a file share witness**. Click **Next**.



Step 6 In the **Configure File Share Witness** screen, specify the path to the File Share. Click **Next**.



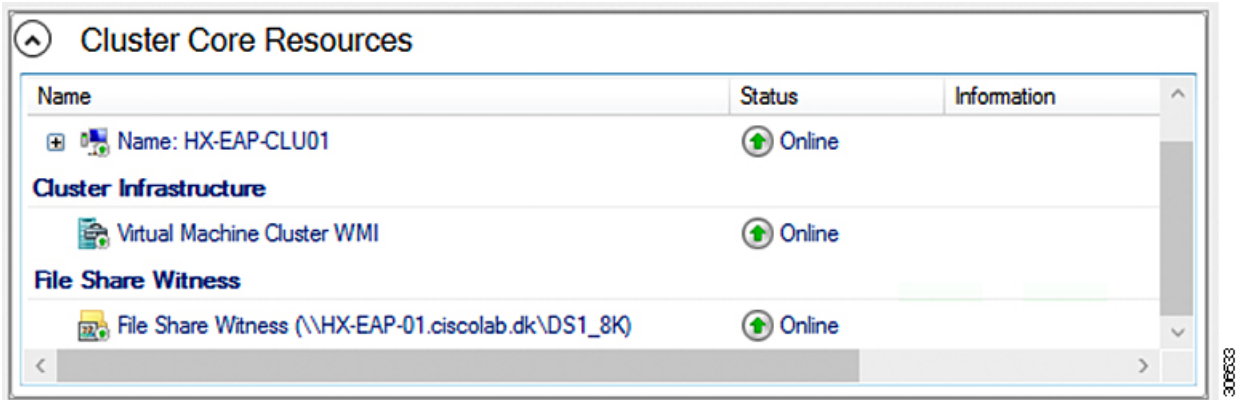
Step 7 In the **Confirmation** screen, click **Next**.



Step 8 In the **Summary** screen, click **Finish** to close the wizard.

Step 9 Alternatively, you can configure a file share witness using Windows PowerShell.

- a) Open a Windows PowerShell console as an administrator.
- b) Type **Set-ClusterQuorum -FileShareWitness <File Share Witness Path>**
- c) You should now see the File Share Witness configured for your cluster. When you navigate to your File Share Witness share you will see a folder created for your cluster.



Checking the Windows Version on the Hyper-V Host

Follow the steps below to check the version of Windows installed.

Step 1 Login to the Hyper-V server as an administrator or HX Service Administrator account.

Step 2 In Powershell, run the following command:

```
C:\Users\adminhyperflex> Get-ItemProperty 'HKLM:\SOFTWARE\Microsoft\Windows NT\CurrentVersion'
```

Step 3 Verify the installed Windows version in the result of the command output.

Following is a sample output if you have installed Windows Server 2016.

```
ProductName : Windows Server 2016 Datacenter
ReleaseId   : 1607
SoftwareType : System
UBR         : 447
```

Step 4 In addition, verify the following:

- For Windows Server 2016 Datacenter Core and Desktop Experience, the Windows 2016 ISO image should be Update Build Revision (UBR) 1884 at a minimum. If not, upgrade the HyperV servers to the latest update. Refer to the *Microsoft Knowledge Base article: KB4467691*.
- If you are using a standalone Hyper-V manager outside HX nodes, then the Hyper-V management server should have a version UBR number greater than 1884. You must upgrade the Hyper-V management server if the version is 1884 or lower.
- For Windows Server 2019 Desktop Experience, the Windows 2019 ISO image should be Update Build Revision (UBR) 107 at a minimum.

Deploying VMs on a Hyper-V cluster

Deploying VMs on a Hyper-V cluster is a multi-step process as described below:

- **Install Remote Server Administration Tools (RSAT) on the management station/host**—You must install administrator tools such as Hyper-V Manager and Failover Cluster Manager as features Server Manager. For more information see, [Install RSAT tools on the Management Station or Host, on page 40](#).
- **Manage VMs**—Connecting to all the Hyper-V nodes in the HX cluster and creating new VMs can be accomplished using either Hyper-V Manager or Failover Cluster Manager. For more information see, [Creating VMs using Hyper-V Manager, on page 45](#).

Install RSAT tools on the Management Station or Host

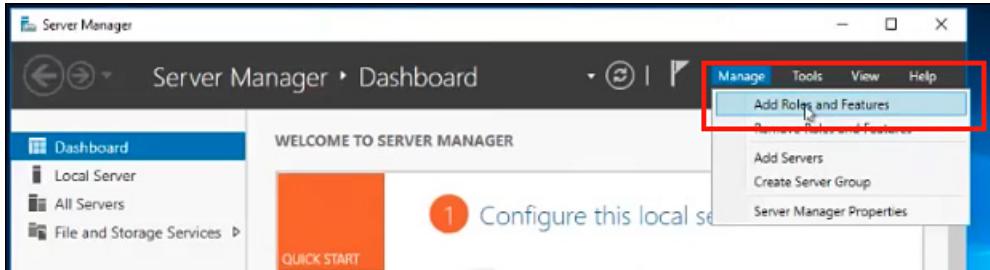
To install RSAT, complete the following steps:

Before you begin

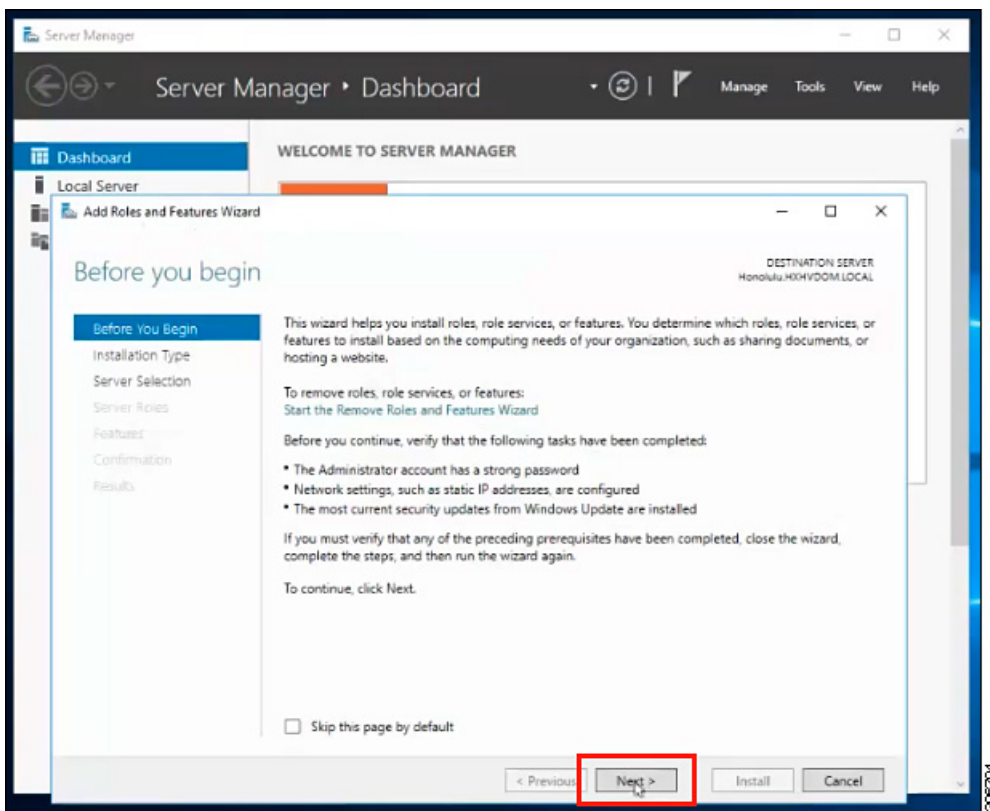
RSAT tool installation requires the following:

- A server from which you can install, manage, monitor the VMs on the Hyper-V HX cluster.
- Administrator tools such as Hyper-V Manager, FCM, PowerShell, SCVMM.

Step 1 In Server Manager, click **Manage** and then select **Add Roles and Features**. The **Add Roles and Features** wizard appears.



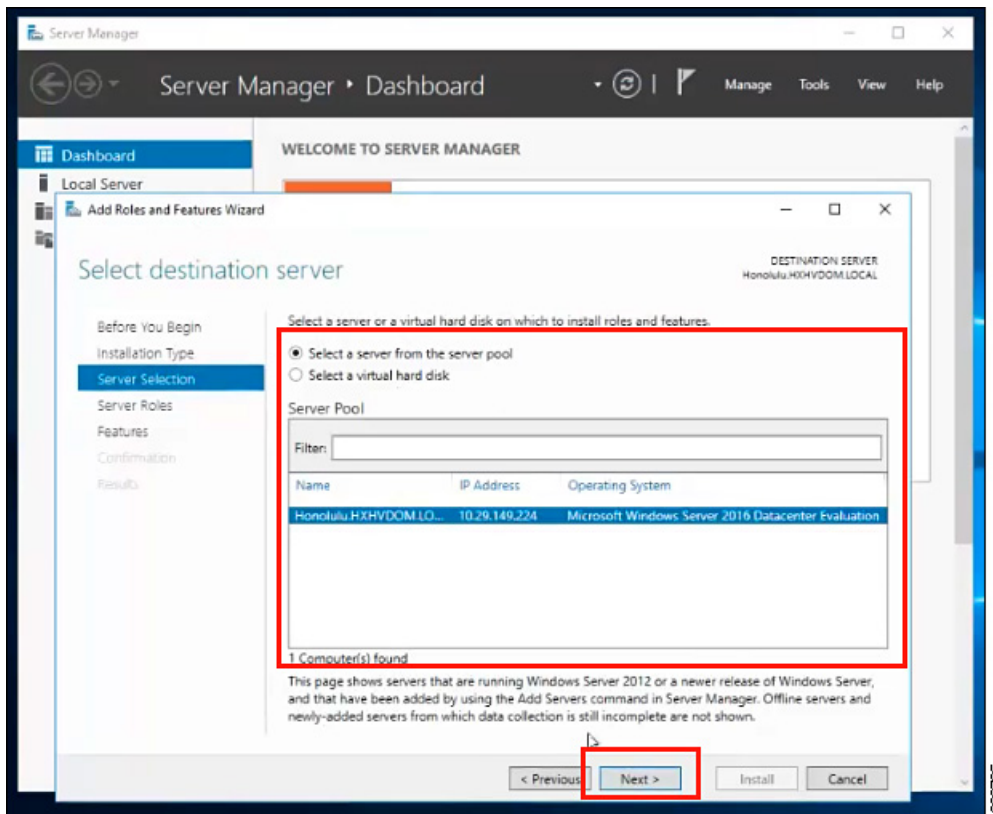
Step 2 In the **Before you begin** page, click **Next**.



Step 3 In the **Select installation type** page, select **Role-based or feature-based installation**. Click **Next**.

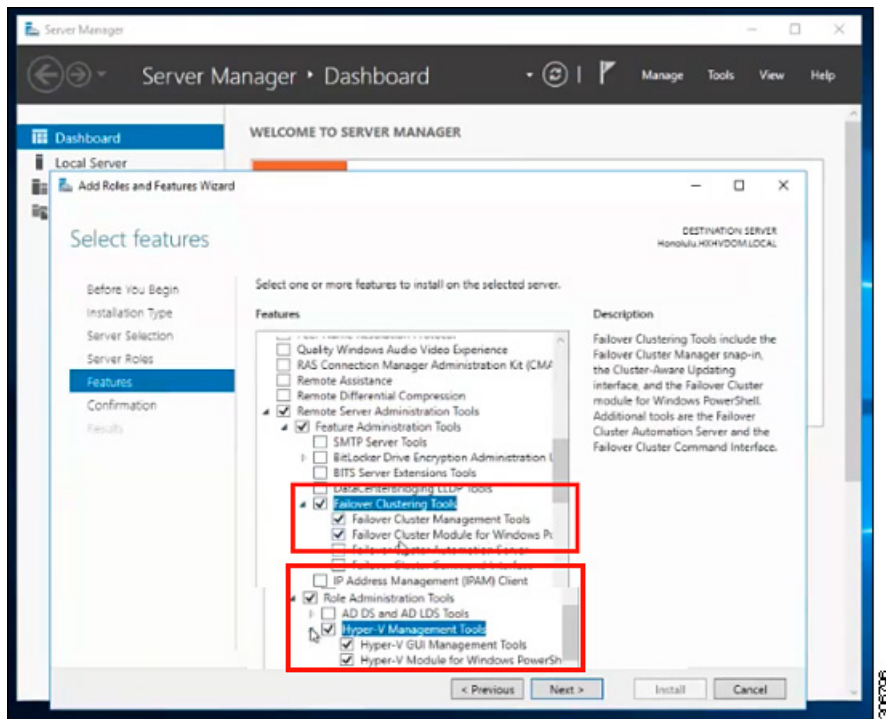
Step 4 In the **Server Selection** page, select your server from the list. This server belongs to the same domain as the HX cluster. Click **Next**.

Install RSAT tools on the Management Station or Host

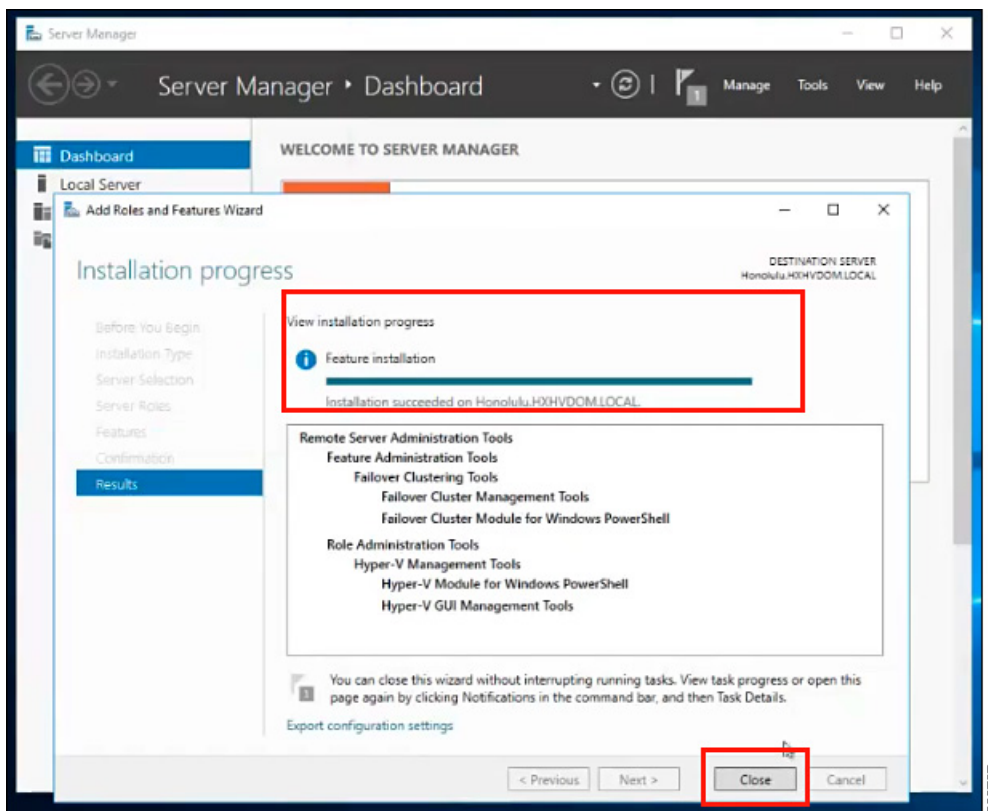


Step 5 In the **Select Roles** page, click **Next**.

Step 6 In the **Features** page, select **Remote Server Administration Tools > Feature Administration Tools > Failover Clustering Tools**, and **Role Administration Tools > Hyper-V Management Tools > Failover Clustering Tools**. Click **Next**.



- Step 7** In the **Confirmation** page, click **Install**. Leave the **Restart the destination server if required** checkbox unchecked.
- Step 8** The **Installation Progress** page displays installation progress. When installation completes, click **Close** to exit the wizard.



Managing VMs using Hyper-V Manager

Connecting to Hyper-V Nodes

Complete the following steps to connect to all the Hyper-V nodes in the Hyper-V HX Cluster.

- Step 1** Open the **Server Manager** dashboard and click **Tools**. Then, click **Hyper-V Manager**. The **Hyper-V Manager** console appears.
- Step 2** In the left pane, select **Hyper-V Manager** and click **Connect to Server...**
- Step 3** In the **Select Computer** dialog box, select **Another computer** and type in the name of the Hyper-V node (for example, HXHV1) that belongs to the Hyper-V cluster. Click **OK**.
- Step 4** Repeat all of the above steps for each node in the Hyper-V HX cluster.

Note For a fresh installation, the storage controller virtual machine (StCt1VM) is the only virtual machine that appears in **Virtual Machines** pane in the **Hyper-V Manager** console. Virtual machines appear in the list under this pane as they are added in each node. For more information on how to create VMs using Hyper-V Manager, see: [Creating VMs using Hyper-V Manager, on page 45](#)

Creating VMs using Hyper-V Manager

Complete the following steps to create VMs using Hyper-V Manager.

-
- Step 1** Open **Hyper-V Manager**.
 - Step 2** Select the Hyper-V server, and right click and select **New > Create a virtual machine**. The **Hyper-V Manager New Virtual Machine** wizard displays.
 - Step 3** In the **Before you Begin** page, click **Next**.
 - Step 4** In the **Specify Name and Location** page, enter a name for the virtual machine configuration file. The location for the virtual machine click **Next**.
 - Step 5** In the **Specify Generation** page, choose either **Generation 1** or **Generation 2**.
 - Step 6** In the **Assign Memory** page, set the start memory value 2048 MB. Click **Next**.
 - Step 7** In the **Configure Networking** page, select a network connection for the virtual machine to use from a list of existing virtual switches.
 - Step 8** In the **Connect Virtual Hard Disk** page, select **Create a Virtual Hard Disk** page, and enter the name, location and size for the virtual hard disk. Click **Next**.
 - Step 9** In the **Installation Options**, you can leave the default option **Install an operating system later** selected. Click **Next**.
 - Step 10** In the Summary page, verify that the list of options displayed are correct. Click **Finish**.
 - Step 11** In Hyper-V Manager, right-click the virtual machine and click **Connect**.
 - Step 12** In the **Virtual Machine Connection** window, select **Action > Start**.
-

Managing VMs using Failover Cluster Manager

Creating VMs using Failover Cluster Manager

Complete the following steps to connect to the Windows Failover cluster (installed along with the Hyper-V HX cluster) and create new VMs using Failover Cluster Manager.

-
- Step 1** In the **Failover Cluster Manager** console, under the **Actions** pane, click **Connect to Server...**
 - Step 2** In the **Select Cluster** dialog box, click **Browse** to navigate to the Hyper-V HX cluster. Click **OK**.
 - Step 3** In the left pane, click **Roles > Virtual Machines... > New Virtual Machines...**
 - Step 4** In the **New Virtual Machine** dialog box, search and select the Hyper-V node where you wish to create new VMs. Click **OK**. The **New Virtual Machine** wizard appears.
 - Step 5** In the **Before You Begin** page, click **Next**.
 - Step 6** In the **Specify Name and Location** page, choose a name for the VM, and specify the location or drive where the VM will be stored. Click **Next**.
 - Step 7** In the **Specify Generation** page, select the generation of virtual machine you want to use (Generation 1 or Generation 2) and click **Next**.
 - Step 8** In the **Assign Memory** page, enter the amount of memory that you want for the VM. Click **Next**.
 - Step 9** In the **Connect Virtual Hard Disk** page, enter the name, location and hard drive size. Click **Next**.
 - Step 10** In the **Installation Options** page, select the install location for the OS. Click **Next**.
 - Step 11** In the **Summary** page, review the options selected and click **Finish**.
 - Step 12** Right-click on the newly created VM, and click **Connect...** In the **Virtual Machine Connection** window, click **Start**.

Note By default, the Failover Cluster Manager will assign a default name for the 4 networks created. It is recommended to rename these network names.

What to do next

To enable redirection of datastore access requests from outside the HX cluster boundary through the management path, add the following entry to the hosts file on the (remote) machine running Hyper-V manager, Failover Cluster Manager, or SCVMM Console. For example, edit `C:\Windows\System32\drivers\etc\hosts` and add:

```
cluster_mgmt_ip \\smb_namespace_name\datastore_name
10.10.10.100 \\hxcluster.company.com\ds1
```

Configuring HyperFlex Share to SCVMM

Before you begin

Edit the `/etc/hosts` file on the host running the VMM admin console to resolve the **smb** access point to the cluster management IP address of HyperFlex cluster. This IP address is typically used to launch Cisco HX Connect.

The complete path is : `C:\Windows\System32\drivers\etc`
Open the "hosts" file in the above directory in Notepad or any other text editor and add the following entry in the bottom :

```
<CMIP> <smb_share_namespace>
```

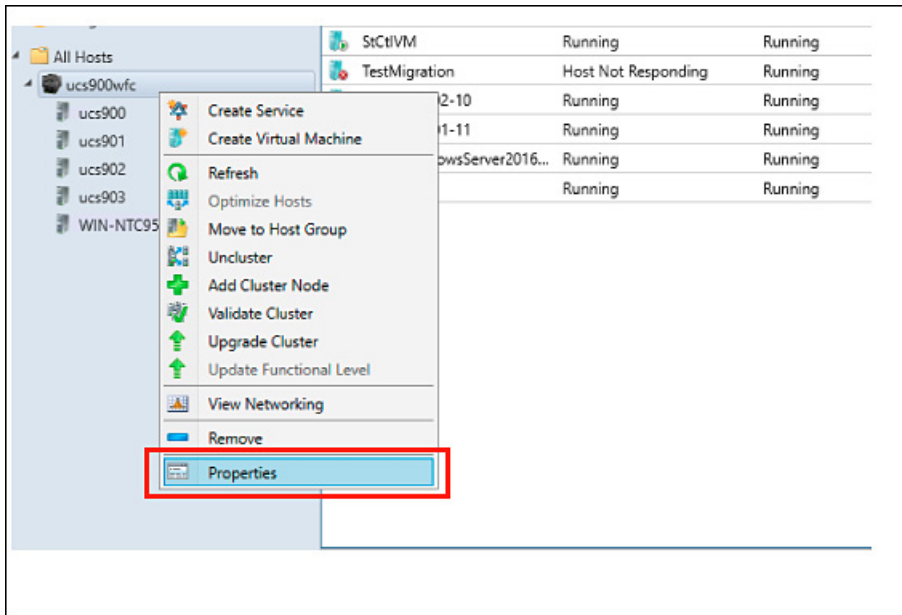
CMIP will be the Cluster Management IP which is usually used to open HX connect UI.

For example,
10.10.10.1 hxhv smb.example.com



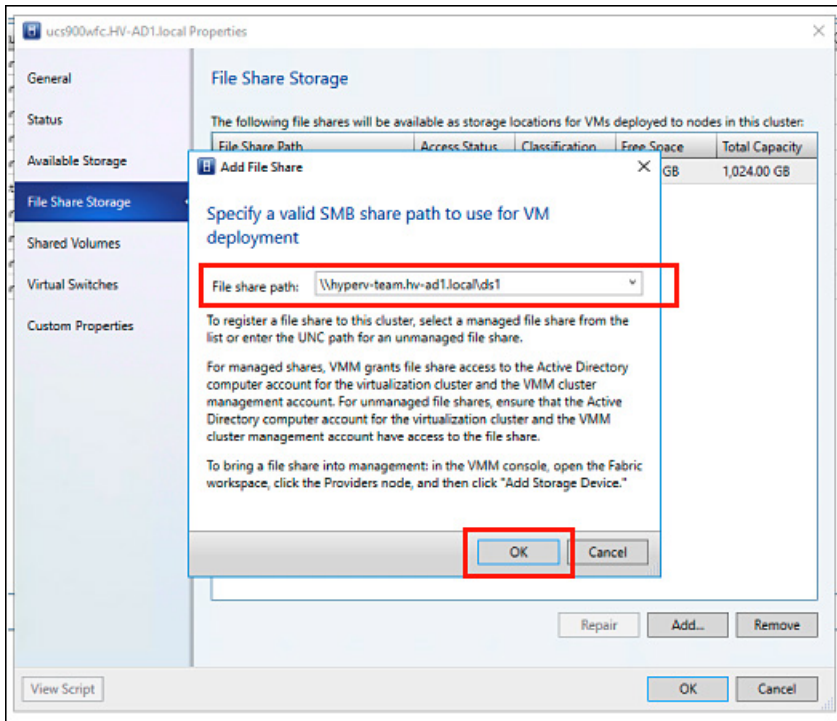
Note For SCVMM Run As account, it is recommended to use **hxadmin** (or any other Domain Admin account which has **FULL** permissions) for the corresponding Hyperflex Organization Unit (OU) in the Active Directory (AD).

- Step 1** Add the cluster to **System Center - Virtual Machine Manager (VMM)**.
- Step 2** In the VMM console, go to **Fabric > Servers > All Hosts**.
- Step 3** Right-click on the cluster and select **Properties**.



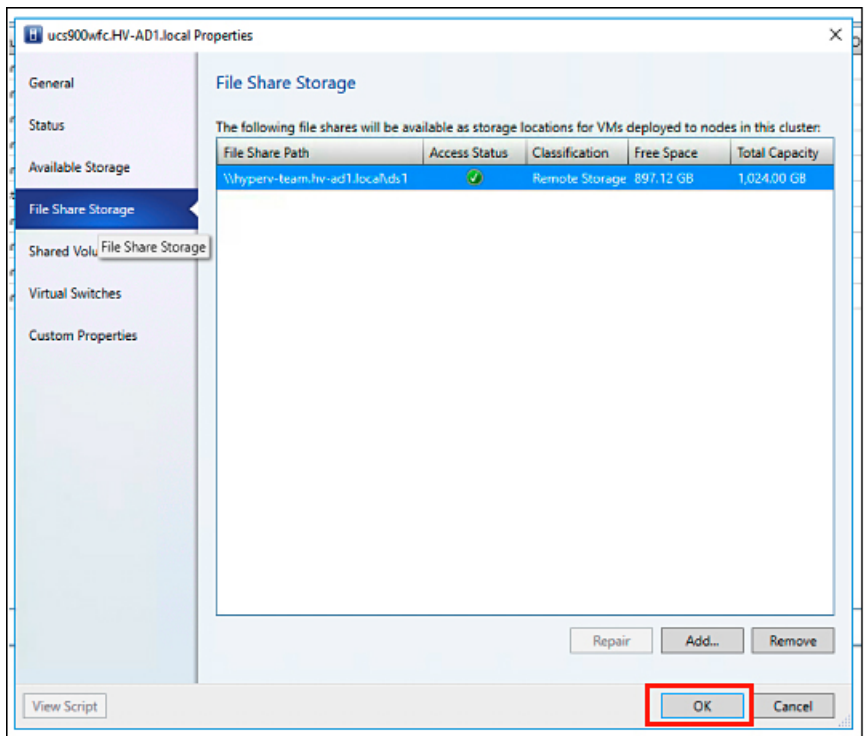
306798

Step 4 In the **Properties** window, right-click **File Share Storage** > **Add File Storage**.



306798

Step 5 When mapping completes, the share is added as shown in the screenshot below.



Step 6 Click **OK** and exit VMM. The HyperFlex Share is now mapped and VMs can be created on this share using SCVMM.

Re-enabling Windows Defender

Run the following commands to re-enable Windows Defender.

Install Defender from PowerShell

```
Install-WindowsFeature -Name Windows-Defender
```

(Optional) Install Defender GUI from PowerShell

```
Install-WindowsFeature -Name Windows-Defender-GUI
```



CHAPTER 5

Appendix

- [Sample Network Configurations, on page 49](#)

Sample Network Configurations

1GE Single Switch

Nexus 5548 using trunk ports

```
vlan 101
  name HX-MGMT
vlan 102
  name HX-STORAGE
vlan 103
  name HX-vmOTION
vlan 104
  name HX-GUESTVM
...
interface Ethernet2/11
  description HX-01-Port1
  switchport mode trunk
  switchport trunk allowed vlan 101-104
  spanning-tree port type edge trunk
  speed 1000
interface Ethernet2/12
  description HX-01-Port2
  switchport mode trunk
  switchport trunk allowed vlan 101-104
  spanning-tree port type edge trunk
  speed 1000
interface Ethernet2/13
  description HX-02-Port1
  switchport mode trunk
  switchport trunk allowed vlan 101-104
  spanning-tree port type edge trunk
  speed 1000
interface Ethernet2/14
  description HX-02-Port2
  switchport mode trunk
  switchport trunk allowed vlan 101-104
  spanning-tree port type edge trunk
  speed 1000
interface Ethernet2/15
  description HX-03-Port1
```

```

switchport mode trunk
switchport trunk allowed vlan 101-104
spanning-tree port type edge trunk
speed 1000
interface Ethernet2/16
description HX-03-Port2
switchport mode trunk
switchport trunk allowed vlan 101-104
spanning-tree port type edge trunk
speed 1000

```

Catalyst 3850-48T using trunk ports

```

vlan 101
name HX-MGMT
vlan 102
name HX-STORAGE
vlan 103
name HX-vMOTION
vlan 104
name HX-GUESTVM
...
interface GigabitEthernet1/0/1
description HX-01-Port1
switchport trunk allowed vlan 101-104
switchport mode trunk
speed 1000
spanning-tree portfast trunk
interface GigabitEthernet1/0/2
description HX-01-Port2
switchport trunk allowed vlan 101-104
switchport mode trunk
speed 1000
spanning-tree portfast trunk
interface GigabitEthernet1/0/3
description HX-02-Port1
switchport trunk allowed vlan 101-104
switchport mode trunk
speed 1000
spanning-tree portfast trunk
interface GigabitEthernet1/0/4
description HX-02-Port2
switchport trunk allowed vlan 101-104
switchport mode trunk
speed 1000
spanning-tree portfast trunk
interface GigabitEthernet1/0/5
description HX-03-Port1
switchport trunk allowed vlan 101-104
switchport mode trunk
speed 1000
spanning-tree portfast trunk
interface GigabitEthernet1/0/6
description HX-03-Port2
switchport trunk allowed vlan 101-104
switchport mode trunk
speed 1000
spanning-tree portfast trunk

```

1GE Dual Switch

Nexus 5548 using trunk ports

This configuration uses DHCP with in-band management using native `vlan 105`. This switch connects to both 1GE LOMs and uses `dhcp relay`.

```
ip dhcp relay
...
interface Vlan105
  ip address 10.1.2.1/24
  ip dhcp relay address 10.1.1.2
  no shutdown
vlan 101
  name HX-MGMT
vlan 102
  name HX-STORAGE
vlan 103
  name HX-vMOTION
vlan 104
  name HX-GUESTVM
vlan 105
  name HX-DHCP-CIMC
...
interface Ethernet2/11
  description HX-01-Port1
  switchport mode trunk
  switchport trunk native vlan 105
  switchport trunk allowed vlan 101-105
  spanning-tree port type edge trunk
  speed 1000
interface Ethernet2/12
  description HX-01-Port2
  switchport mode trunk
  switchport trunk native vlan 105
  switchport trunk allowed vlan 101-105
  spanning-tree port type edge trunk
  speed 1000
interface Ethernet2/13
  description HX-02-Port1
  switchport mode trunk
  switchport trunk native vlan 105
  switchport trunk allowed vlan 101-105
  spanning-tree port type edge trunk
  speed 1000
interface Ethernet2/14
  description HX-02-Port2
  switchport mode trunk
  switchport trunk native vlan 105
  switchport trunk allowed vlan 101-105
  spanning-tree port type edge trunk
  speed 1000
interface Ethernet2/15
  description HX-03-Port1
  switchport mode trunk
  switchport trunk native vlan 105
  switchport trunk allowed vlan 101-105
  spanning-tree port type edge trunk
  speed 1000
interface Ethernet2/16
  description HX-03-Port2
  switchport mode trunk
  switchport trunk native vlan 105
  switchport trunk allowed vlan 101-105
  spanning-tree port type edge trunk
  speed 1000
```

Repeat the same configuration on switch #2. Eliminate the `dhcp relay` and `interface Vlan 105` commands.

Catalyst 3850-48T using trunk ports

This configuration uses statically-assigned CIMC IPs on `vlan 105`. All `vlan`s are allowed on all trunk interfaces. For security purposes, we recommend restricting the VLANs to those required for a HyperFlex deployment by adding the `switchport trunk allowed vlan` statement into all your port configurations.

```
vlan 101
  name HX-MGMT
vlan 102
  name HX-STORAGE
vlan 103
  name HX-vMOTION
vlan 104
  name HX-GUESTVM
vlan 105
  name HX-CIMC
...
interface GigabitEthernet1/0/1
  description HX-01-Port1
  switchport mode trunk
  speed 1000
  spanning-tree portfast trunk
interface GigabitEthernet1/0/2
  description HX-01-Port2
  switchport mode trunk
  speed 1000
  spanning-tree portfast trunk
interface GigabitEthernet1/0/3
  description HX-02-Port1
  switchport mode trunk
  speed 1000
  spanning-tree portfast trunk
interface GigabitEthernet1/0/4
  description HX-02-Port2
  switchport mode trunk
  speed 1000
  spanning-tree portfast trunk
interface GigabitEthernet1/0/5
  description HX-03-Port1
  switchport mode trunk
  speed 1000
  spanning-tree portfast trunk
interface GigabitEthernet1/0/6
  description HX-03-Port2
  switchport mode trunk
  speed 1000
  spanning-tree portfast trunk
```

Repeat the same configuration on switch #2.

10GE Dual Switch

Nexus 9000 using trunk ports

```
vlan 101
  name HX-MGMT
vlan 102
  name HX-STORAGE
vlan 103
  name HX-vMOTION
```



```
vlan 104
  name HX-GUESTVM
vlan 105
  name HX-DHCP-CIMC
...
interface Ethernet1/35
  description M5-Edge-Node1-VIC1
  switchport mode trunk
  switchport trunk native vlan 105
  switchport trunk allowed vlan 101-105
  spanning-tree port type edge trunk

interface Ethernet1/36
  description M5-Edge-Node1-VIC2
  switchport mode trunk
  switchport trunk native vlan 105
  switchport trunk allowed vlan 101-105
  spanning-tree port type edge trunk

interface Ethernet1/37
  description M5-Edge-Node2-VIC1
  switchport mode trunk
  switchport trunk native vlan 105
  switchport trunk allowed vlan 101-105
  spanning-tree port type edge trunk

interface Ethernet1/38
  description M5-Edge-Node2-VIC2
  switchport mode trunk
  switchport trunk native vlan 105
  switchport trunk allowed vlan 101-105
  spanning-tree port type edge trunk

interface Ethernet1/39
  description M5-Edge-Node3-VIC1
  switchport mode trunk
  switchport trunk native vlan 105
  switchport trunk allowed vlan 101-105
  spanning-tree port type edge trunk

interface Ethernet1/40
  description M5-Edge-Node3-VIC2
  switchport mode trunk
  switchport trunk native vlan 105
  switchport trunk allowed vlan 101-105
  spanning-tree port type edge trunk
```

Catalyst 9300 using trunk ports

```
vlan 101
  name HX-MGMT
vlan 102
  name HX-STORAGE
vlan 103
  name HX-vmOTION
vlan 104
  name HX-GUESTVM
vlan 105
  name HX-CIMC
...
interface GigabitEthernet1/0/1
  description M5-Edge-16W9-LOM1
  switchport trunk allowed vlan 101-105
  switchport mode trunk
```

```
spanning-tree portfast trunk

interface GigabitEthernet1/0/2
description M5-Edge-16W9-LOM2
switchport trunk allowed vlan 101-105
switchport mode trunk
spanning-tree portfast trunk

interface GigabitEthernet1/0/3
description M5-Edge-16UQ-LOM1
switchport trunk allowed vlan 101-105
switchport mode trunk
spanning-tree portfast trunk

interface GigabitEthernet1/0/4
description M5-Edge-16UQ-LOM2
switchport trunk allowed vlan 101-105
switchport mode trunk
spanning-tree portfast trunk

interface GigabitEthernet1/0/5
description M5-Edge-05G9-LOM1
switchport trunk allowed vlan 101-105
switchport mode trunk
spanning-tree portfast trunk

interface GigabitEthernet1/0/6
description M5-Edge-05G9-LOM2
switchport trunk allowed vlan 101-105
switchport mode trunk
spanning-tree portfast trunk
```